GRC
GENDARMERIE ROYALE DU CANADA

AU SERVICE DE LA COMMUNAUTÉ POLICIÈRE DEPUIS 1939

GAZETTE

GAGNANT DU PRIX OR MARCOM 2016

VOL.79, N° 3, 2017

CYBERCRIMINALITÉ
SAISIE D'ÉLÉMENTS DE PREUVE ET MISE EN ÉCHEC DES DÉLINQUANTS

ENQUÊTE SUR LES CYBERCRIMES
BRIGADE CHARGÉE DES AFFAIRES LES PLUS GRAVES P. 7

TRIAGE DE LA PREUVE NUMÉRIQUE
COMMENT LA FAIRE PARVENIR VITE À L'ENQUÊTEUR P. 16

CHASSEUR DE PRÉDATEURS
UN EXPERT ENTIÈREMENT DÉVOUÉ À LA CAUSE P. 19

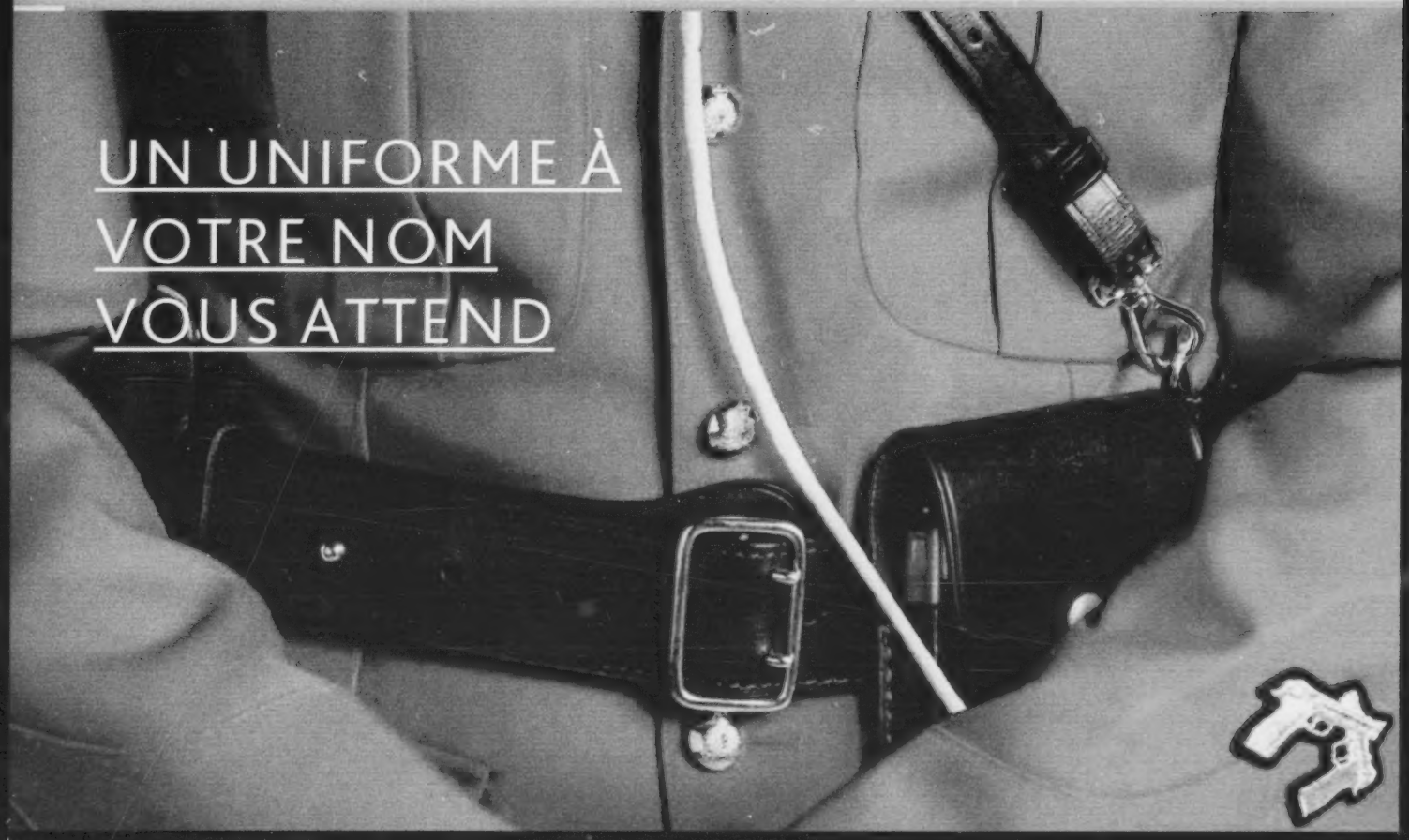
RCMP-GRC.GC.CA

Gendarmerie royale du Canada | Royal Canadian Mounted Police

Canada

GRC

GENDARMERIE ROYALE DU CANADA



DE LA REMISE DES DIPLÔMES À L'ACTION

Après avoir réussi votre formation à l'École de la Gendarmerie royale du Canada, vous commencerez immédiatement votre carrière policière.

carrieresgrc.ca

Gendarmerie royale du Canada | Royal Canadian Mounted Police

Canada

GAZETTE

Au service de la communauté policière depuis 1939

Vol. 79, N° 3, 2017

Une publication de la Gendarmerie royale du Canada

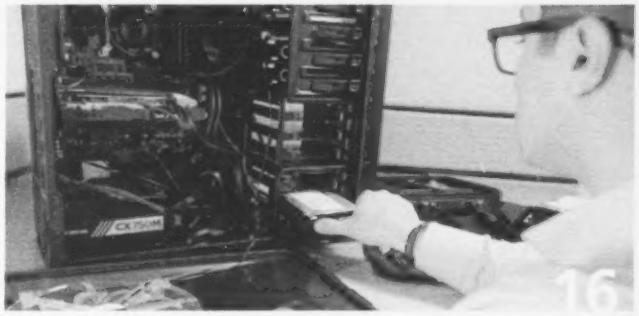
DOSSIER

7 Une escouade de la cybercriminalité priorise les cas majeurs
10 Interprétation de données par les experts en criminalistique numérique
12 Débat de spécialistes : quel est le défi de la répression de la cybercriminalité?
14 Un groupe du cyberrenseignement recueille des données à l'appui d'enquêtes
15 Des cours à l'intention des enquêteurs en cybercriminalité
16 Le triage sur place accélère le traitement d'éléments de preuve numériques
17 Atelier de sensibilisation à la technologie à l'intention des agents sur le terrain
18 Nouvelle technologie : la GRC en quête d'un logiciel apte à repérer les images d'exploitation sexuelle d'enfants
19 Entretien : un expert en communication secrète traque les prédateurs du Web

RUBRIQUES

4 Éditorial
5 Actualités
20 Les faits : le vol de véhicules en bref
21 Avis d'un expert : les données de communication interprétées par un spécialiste
22 Dernières tendances : une seconde carrière dans la police
23 Pratique exemplaire : mettre fin à la conduite dangereuse de VTT
24 À l'avant-scène
26 Dernière page : surmonter les épreuves

EN COUVERTURE :
Savoir-faire technique et solides compétences d'enquête sont de puissants outils de lutte contre la cybercriminalité. Photo : Serge Gouin, GRC



SUR LA VOIE DE LA « CYBERCOMPÉTENCE »

Serge Gouin, GRC

Le rançongiciel de portée mondiale qui a récemment touché des centaines de milliers de personnes illustre bien ce que les services de police savent déjà : les cybercrimes sont de plus en plus fréquents et de plus en plus graves.

En 2015, la GRC a mis en place sa stratégie anti-cybercriminalité, qui vise à réduire les risques de délits informatiques ainsi que l'incidence et le nombre de victimes de ces délits au Canada.

Le présent numéro montre comment la GRC maintient l'ordre et le droit à l'ère du numérique.

Dans l'article principal, Deidre Seiden, qui a vu à Ottawa l'Équipe d'enquête sur les cybercrimes de la GRC faire avancer une affaire en cours depuis des mois, décrit le fonctionnement de la nouvelle équipe et le rôle qu'elle joue dans une perspective nationale et mondiale.

La valeur d'une enquête tenant à celle des renseignements recueillis, le Centre national de coordination du renseignement a mis sur pied une équipe de cyberrenseignement ayant pour tâche de rassembler de l'information et de repérer les possibilités d'action pour les groupes d'enquête. L'équipe cible les pirates informatiques et suit leurs empreintes numériques.

Sur le versant criminalistique des délits informatiques, M^me^ Seiden découvre comment les groupes de la criminalité technologique contribuent aux enquêtes par la saisie et le traitement des éléments de preuve numériques – une expertise capitale à l'heure des progrès technologiques ultrarapides.

La technologie devenant accessible à de plus en plus de gens, y compris des criminels, le besoin de telles unités spécialisées croît en flèche. Pour gérer ce fort volume de travail, la GRC a, en Colombie-Britannique, lancé un programme de triage sur place de la preuve numérique. Le programme enseigne à des non-spécialistes comment savoir si un appareil contient ou non des éléments de preuve avant son envoi au service d'analyse judiciaire, où les délais sont longs. Le triage sur place met rapidement des informations probantes entre les mains des enquêteurs.

Technophiles ou non, les policiers de première ligne doivent suivre l'évolution de la technologie et du droit qui s'y rapporte. Amelia Thatcher écrit au sujet du Cybercrime Investigations Workshop, un cours intensif sur les crimes informatiques et technologiques donné en Nouvelle-Écosse. Le cours d'une journée fournit aux policiers les connaissances et les outils pas-à-pas dont ils ont besoin pour enquêter sur ce type d'affaires.

C'est une tâche colossale que celle de repérer les images d'exploitation juvénile et d'arrêter les prédateurs en ligne, et quand une infraction est en cours, une intervention immédiate s'impose.

La GRC recourt à l'intelligence artificielle pour analyser et repérer, parmi des millions de photos, celles qui sont le plus susceptibles d'être illicites. L'algorithme utilisé élimine les images innocentes et place en tête de liste celles qui, potentiellement, le sont le moins. Cela fait gagner du temps en plus de réduire l'exposition des policiers à des images obscènes et choquantes.

À côté des outils technologiques, conçus pour les tâches fastidieuses et difficiles, certaines méthodes reposent toujours sur le contact humain, comme celle du cap. Jared Clarke, expert en communication secrète habitué à se faire passer pour une victime potentielle ou un prédateur en ligne. Son engagement a sauvé des dizaines de jeunes victimes des griffes d'un agresseur.

Le présent numéro n'est pas qu'un rappel de la nécessité de suivre le rythme de l'internetisation rapide de la société : il souligne l'impératif d'employer des méthodes policières astucieuses – dans un monde où ordinateurs et téléphones intelligents permettent de tout faire ou presque. ■

— Katherine Aldred

GAZETTE

ÉDITRICE : Nancy Sample

RÉDACTRICE EN CHEF : Katherine Aldred

RÉDACTRICES : Deidre Seiden, Amelia Thatcher

ÉDITEUR WEB : Richard Vieira

GRAPHISME : Lisa McDonald-Bourg

TRADUCTION : Services de traduction de la Direction générale, GRC

IMPRIMERIE : St. Joseph Communications

La *Gazette* (ISSN 1196-6513) est publiée en versions française et anglaise par la Direction des services de communication nationaux de la Gendarmerie royale du Canada, à Ottawa. La conception de la page couverture ainsi que les articles sont protégés par les droits d'auteur et aucune partie de cette revue ne peut être reproduite sans consentement écrit. Poste-publication, numéro de convention 40064068. La *Gazette* paraît quatre (4) fois par année et est distribuée gratuitement mais en nombre restreint aux services de police et aux organismes d'exécution de la loi. On conseille fortement de la faire circuler. On ne peut pas s'y abonner à titre personnel.

On vous prie de faire parvenir vos lettres, articles et commentaires à la rédactrice en chef de la *Gazette*. La rédaction se réserve le droit de faire la révision. © 2017 GRC.

POUR COMMUNIQUER AVEC NOUS :

Gazette de la GRC
73, promenade Leikin
MB-1, pièce 801
Ottawa (Ontario) K1A 0R2
CANADA

Téléphone : 613-843-4570
Courriel : gazette@rcmp-grc.gc.ca
Internet : www.rcmp-grc.gc.ca/gazette

RESTEZ AU COURANT AVEC LA GRC

Visitez notre site Internet : **www.rcmp-grc.gc.ca**

Suivez-nous sur Facebook : **www.facebook.com/grcrcmp**

Suivez-nous sur Twitter : **@grcrcmppolice #gazettegrc**

Visualisez nos vidéos sur YouTube : **www.youtube.com/rcmpgrcpolice**

L'ADOPTION D'UN NOUVEAU SYSTÈME RADIO

par Deidre Seiden

Au Nouveau-Brunswick, l'utilisation d'un langage radio codé était de mise pour les policiers afin de maintenir la confidentialité des appels devant la menace d'écoute clandestine par scanneur.

« Nous pensions déjouer les gens en utilisant les codes 10, explique le s.é.-m. Jamie Melanson, chef de veille dans la région de Codiac. Mais tout le monde sait ce que veut dire 10-4. Les codes sont expliqués dans Internet. Il n'y a plus de mystère. »

Pour contourner le problème, les répartiteurs ont commencé à transmettre les appels de façon électronique, ce qui était efficace, mais seulement lorsque les membres étaient dans leur autopatrouille, où ils avaient accès à leur ordinateur.

La solution : un nouveau système radio.

En collaboration avec le gouvernement provincial, les policiers et les premiers intervenants au Nouveau-Brunswick ont commencé à utiliser le système radio mobile à commutation automatique de canaux. Le lancement a débuté en 2017 et se poursuivra graduellement tout au long de l'année.

« Il nous faut retirer toutes les anciennes radios des voitures et des détachements, précise Shawn Vautour, directeur de la station des transmissions opérationnelles et du projet de renouvellement des radios. C'est une tâche énorme, mais le jeu en vaut la chandelle. »

Le nouveau système est entièrement numérique et chiffré. Plus besoin de codes 10 : les policiers peuvent s'exprimer en langage clair.

En outre, le système interconnecté permet d'aplanir les barrières dans les communications à l'échelle de la GRC, entre les provinces voisines et entre les partenaires.

« C'est très stimulant, explique M. Vautour. Le système fonctionne comme un téléphone; un membre dans le nord de la province peut parler à un collègue dans le sud intervenu sur les lieux d'un incident. Tous les secteurs du Nouveau-Brunswick, de la Nouvelle-Écosse et de l'Île-du-Prince-Édouard peuvent communiquer entre eux, ce qui favorise la connaissance de la situation. »

GRC

La GRC au Nouveau-Brunswick lance un nouveau système radio entièrement chiffré, pour une interopérabilité accrue entre les partenaires et les provinces avoisinantes.

Et pour la première fois, les policiers peuvent contacter d'autres intervenants dans la province.

« Il en va de la sécurité publique, explique le s.é.-m. Melanson. Grâce à cette avancée technologique, les différents intervenants peuvent répondre à un appel simultanément. Tout le monde y gagne. » ■

LE PUBLIC APPELÉ À RECONNAÎTRE DES VISAGES À RICHMOND

par Amelia Thatcher

La GRC de Richmond a lancé son nouveau site Web *Richmond Help Identify* et encourage les résidants à jouer les détectives pour l'aider à reconnaître des personnes d'intérêt qu'elle a été jusqu'ici incapable d'identifier.

Dans l'espoir de classer certaines affaires, le détachement demande aux membres du public si des visages sont familiers.

« Dans notre métier, on ne connaît pas tout le monde. On espère donc que les citoyens puissent reconnaître un visage ou demandent l'aide de leurs amis, dit le serg. Gene Hsieh, chef du groupe de la réduction de la criminalité au Dét. de Richmond. L'idée est de tirer profit des médias sociaux et du désir de la population d'élucider des crimes. »

On publie régulièrement sur le site Web de nouvelles photos prises par des caméras de surveillance de propriétaires et même des portraits robots. Pour chaque suspect, on indique le sexe, la date de publication de la photo et le crime dont il est soupçonné.

Le détachement encourage quiconque reconnaît un visage dans le site Web à lui téléphoner ou à lui envoyer l'information par courriel.

« L'un des plus importants éléments du travail policier, ce sont les indices, précise le cap. Dennis Hwang, un agent de communication qui a contribué à la création du site. Un nom est un bon point de départ. Mais sans indice, l'affaire reste non résolue. »

Ces dernières années, le coût des systèmes de surveillance résidentielle a baissé, tandis que la qualité des vidéos s'est améliorée. D'après le cap. Hwang, cette tendance a engendré un afflux d'images de criminels au détachement. Mais la police ne peut pas toujours les identifier.

« Nous avons un excédent de photos et avant, nous n'en tirions pas profit, confie le cap. Hwang. Aujourd'hui, grâce au site, le public peut nous aider à clore des dossiers. »

Depuis le lancement du site en novembre 2016, des renseignements obtenus de la population ont permis d'identifier trois suspects. Des enquêtes sont en cours relativement à ces affaires.

GRC de Richmond

Afin d'intéresser le public à son nouveau site Web, *Richmond Help Identify*, le détachement publie sur Twitter tout nouveau visage non identifié.

« Nous voulons résoudre toutes les affaires, quelles qu'elles soient, lance le serg. Hsieh. Même si nous n'identifions qu'un suspect, c'est un exploit que nous n'aurions pas pu réaliser autrement. » ■

SYSTÈME DE LA POLICE DE DELTA POUR SUIVRE LES FUYARDS

par Deidre Seiden

À Delta, banlieue de Vancouver (C.-B.), les criminels peuvent échapper à la police, mais ne peuvent aller bien loin.

Le service de police de Delta a installé, sur huit de ses véhicules, un outil de gestion des poursuites (GPS) qui permet aux policiers de suivre les véhicules qui refusent de s'immobiliser.

Les policiers devaient composer avec une hausse considérable du nombre de refus de s'immobiliser. En 2016, on comptait 70 cas où les suspects ont échappé à la police.

En cherchant une solution, le service est tombé sur l'outil StarChase Pursuit Management.

« Notre priorité est la sécurité du public, dit le gend. Andrew Cortes, gestionnaire de projet pour la nouvelle technologie. Nous avions besoin d'un moyen d'arrêter ces conducteurs et de réduire le risque pour le public, les policiers et les délinquants eux-mêmes. Les fuyards conduisent moins dangereusement s'ils pensent que la police ne les poursuit pas. »

L'outil permet aux policiers de lancer un « dard » GPS, de la taille d'une canette, du grillage avant du véhicule de police sur un véhicule suspect.

Une fois que le GPS adhère au véhicule, les policiers peuvent ralentir. C'est le centre de répartition qui suit le véhicule et transmet l'information aux policiers.

« Nos membres ont le temps d'élaborer un plan d'approche coordonnée pour arrêter le délinquant lorsque le véhicule est immobilisé », dit-il.

Le gend. Jim Ingram de la police de Delta a été formé pour utiliser le nouvel outil et a été le premier à s'en servir. Cette fois-là, il a lancé le dard par précaution, même si le conducteur s'était arrêté.

« Si on pense qu'un conducteur pourrait prendre la fuite, comme un vendeur de drogue sur appel, on le marque et on tente ensuite de faire un contrôle routier, dit-il. C'est frustrant de laisser les criminels nous échapper, mais maintenant, on peut les retrouver. » ■

La police de Delta a un nouvel outil de gestion de poursuite, un GPS qui permet de suivre les véhicules qui ne se sont pas immobilisés.

Service de police de Delta

CARRIOLES DE SAUVETAGE AU MANITOBA

par Amelia Thatcher

Dans deux communautés nordiques du Manitoba, la GRC a un nouvel outil de sauvetage : une remorque tout-terrain pour les criminels et les habitants en détresse.

Avec des skis et des roues interchangeables, les carrioles couvertes s'accrochent à l'arrière de motoneiges ou de véhicules tout-terrain (VTT) et peuvent transporter deux personnes. Elles ressemblent aux remorques pour enfant tirées par des vélos, mais sont mieux équipées.

« Chauffées et éclairées, elles peuvent être utilisées toute l'année, dit le serg. Joe Frizzley, chef du Détachement de la GRC à Thompson (Man.), tant pour l'application de la loi que pour les urgences. »

Les détachements de la GRC à The Pas et à Thompson (Man.) ont acheté chacun une carriole en février dernier. Selon le s.é.-m. Brent Mattice, chef du Détachement de The Pas, l'idée est venue des services d'urgence locaux, qui utilisent une carriole similaire comme ambulance tout-terrain.

« Tout d'abord, si une personne est blessée dans une région éloignée, on peut la placer dans la carriole et emprunter le chemin le plus direct pour la ramener, dit-il. C'est complètement couvert, les passagers sont donc protégés contre les éléments. »

Jusqu'à maintenant, on utilisait un traîneau ouvert pour transporter ces personnes. La nouvelle carriole permet de transporter les blessés de façon plus sécuritaire et dans un plus grand confort.

Il explique que les carrioles seront également utilisées lors d'accidents de motoneige et de VTT dans la brousse. L'alcool étant souvent en cause, les détachements avaient besoin d'un moyen de transport pour ceux qui étaient accusés de conduite avec facultés affaiblies.

« Si une personne est arrêtée, nous pouvons l'asseoir en toute sécurité dans la carriole et la ramener au poste pour un alcootest », dit-il.

Le serg. Frizzley dit que les carrioles peuvent aussi servir à transporter de l'équipement et des appareils électroniques de nature délicate dans des lieux de crime éloignés.

Elles n'ont pas encore été utilisées, mais le serg. Frizzley et le s.é.-m. Mattice sont convaincus qu'elles seront un outil intégral de leur service.

« Certains lieux se trouvent au milieu de nulle part, dit le serg. Frizzley. Surtout dans le Nord, c'est un moyen pour nous de secourir les personnes. » ■

Les nouvelles carrioles peuvent être remorquées par des motoneiges à l'hiver et des VTT à l'été si l'on remplace les skis par des roues.

Cpl. Colin Stark, GRC

Serge Gouin, GRC

L'Équipe d'enquête sur la cybercriminalité se consacre à la répression de la cybercriminalité touchant les infrastructures essentielles et du gouvernement canadien.

L'UNION FAIT LA FORCE

UNE NOUVELLE ÉQUIPE S'ATTAQUE À LA CYBERCRIMINALITÉ

par Deidre Seiden

L'heure est critique pour l'Équipe d'enquête sur la cybercriminalité (EEC) de la GRC. On est vendredi, dernière journée de travail de l'escouade avant de quitter la ville pour exécuter un mandat de perquisition et arrêter un suspect dans sa plus récente enquête.

*Le gend. Falardeau, déposant chargé de rédiger le mandat de perquisition nécessaire à l'enquête, passe voir *le serg. Beaulieu, s.-off. des opérations de l'EEC, afin de recevoir les dernières instructions pour l'instance au tribunal.

« Il nous faut faire signer ce mandat par un juge aujourd'hui, explique le gend. Falardeau. C'est une pièce essentielle du casse-tête. »

Depuis ce matin, les membres de l'équipe défilent l'un après l'autre devant le serg. Beaulieu pour lui poser des questions de dernière minute sur l'affaire.

« C'est la partie stimulante, constate-t-il. Depuis trois mois, nous faisons notre travail en recueillant des éléments de preuve contre le suspect, et nous sommes maintenant prêts à l'appréhender. »

UNE ÉQUIPE NOUVELLE CHARGÉE D'UNE STRATÉGIE INÉDITE

Pendant des années, la GRC a mis la priorité aux menaces cybercriminelles, enquêtant sur celles-ci, les perturbant et gérant les preuves numériques à l'appui des enquêtes, mais l'EEC est la première équipe spécialisée en cybercriminalité stricte au pays.

Situé à la Division nationale de la GRC à Ottawa, ce groupe de pointe a vu le jour en 2015 avec le mandat d'enquêter sur les crimes ciblant l'ordinateur et la technologie.

Sa création est une étape déterminante dans la stratégie de la GRC pour réprimer la menace et la victimisation liées à la cybercriminalité.

« Ses membres sont l'élément pointu de la stratégie », explique le surint. Denis Desnoyers, officier responsable des enquêtes criminelles à la Division nationale.

Si de telles équipes existent déjà dans de nombreux pays, le Canada est en mesure de tirer profit des leçons apprises.

« N'ayant pas à réinventer la roue, notre équipe dispose d'une longueur d'avance », souligne le surint. Desnoyers.

À l'origine, c'étaient les groupes de la criminalité technologique (GCT), répartis à l'échelle du pays, qui étaient théoriquement chargés d'enquêter sur la cybercriminalité. Mais en raison de leur charge de travail, c'était rarement le cas dans les faits. Ils soutenaient plutôt les enquêtes en assumant une expertise judiciaire numérique.

Une fois mise sur pied, l'EEC s'est chargée des affaires les plus graves. Il s'agit de dossiers retentissants de portée internationale, de nature délicate ou qui touchent des infrastructures essentielles ou du gouvernement fédéral.

Le s.é.-m. Maurizio Rosa est le s.-off. resp. du GCT à la Division nationale. L'EEC relève du GCT, qui comprend aussi l'équipe

d'expertise judiciaire numérique.

Le s.é.-m. Rosa a joué un rôle crucial dans la constitution de l'équipe. D'emblée, il savait la forme qu'il voulait lui donner, fort de son expérience des enquêtes générales et de l'expertise judiciaire numérique.

Son but : allier des enquêteurs férus de technologie à d'autres rompus aux méthodes traditionnelles d'enquête.

Il a donc évalué les candidats en fonction de leurs antécédents pour former une équipe aux compétences complémentaires.

Chaque volet de l'équipe a sa fonction : le volet d'enquête qui assume le travail policier conventionnel lié aux cyberinfractions, et le volet d'expertise judiciaire numérique traitant les données à l'appui des accusations envisagées.

« Il s'agit d'un modèle efficace, soutient le s.é.-m. Rosa. Notre équipe fait preuve d'un moral, d'une éthique de travail et d'un esprit d'initiative solides. »

À sa troisième et dernière année de développement, l'équipe a atteint la taille critique. L'enquête dont elle est actuellement chargée est la première où des accusations sont imminentes.

BREFFAGE

Peu avant 10 h, le serg. Beaulieu se dirige vers la salle de réunion et prend place à la table pour un dernier breffage à Ottawa.

Malgré la pression, l'atmosphère est détendue tandis que les membres de l'équipe d'enquête attendent le début de la séance.

L'enquêteur principal dans l'affaire, *le gend. Veilleux, entre et capte l'attention de l'auditoire.

Il passe d'abord en revue les détails du projet, énumérant les activités du suspect, ses associés connus et les lieux où il prend son souper, en priant les membres de les éviter.

Chaque détail a été analysé.

« Dans un cas de ce genre, nous n'avons droit à aucune marge d'erreur », précise le gend. Veilleux.

Les enquêtes cybercriminelles sont une discipline relativement nouvelle à la GRC, tout comme dans la jurisprudence. De fait, peu de cas ont répondu aux critères des tribunaux.

« Notre responsabilité est grande, explique le s.é.-m. Rosa. Nous devons nous fier aux techniques d'enquête déployées, tout en veillant à le faire de façon à résister à l'examen des tribunaux. »

Le gend. Veilleux passe en revue une vaste liste d'éléments à saisir, dont des ordinateurs, des portatifs et des cellulaires, ainsi que des relevés bancaires et des documents relatifs à certains sites Web.

Il ne sait pas avec précision combien d'ordinateurs et de cellulaires le suspect possède; mais il sait que ce dernier en a mis un en vente en ligne.

« Avons-nous tenté de l'acheter ? », dit un membre à la blague.

Le gend. Veilleux conclut en rappelant que la sécurité de chacun lui importe au plus haut point. « Nous devons être solidaires du début à la fin de l'opération. »

C'est un rappel que toute enquête, cybercriminelle ou non, comporte des risques.

UNE CRIMINALITÉ SANS FRONTIÈRES

Les crimes traditionnels, comme les vols de banque, présentent souvent un élément de risque. Ces infractions physiques, violentes posent un danger pour le public, les policiers, voire les criminels eux-mêmes.

Dans le cyberespace, un acteur peut se retrancher dans l'anonymat.

« La cybercriminalité est en hausse, souligne le s.é.-m. Rosa. Chaque possibilité qui atténue les risques tout en optimisant le profit sera exploitée. »

Le malfaiteur ne connaît peut-être pas sa victime, mais ses actes ont une incidence sur le plan personnel et au niveau national ou mondial.

« Lorsqu'il est question de données informatiques et de cybercriminalité, les frontières n'existent pas, explique le serg. Beaulieu. Leur mobilité est entière. »

La lutte contre la cybercriminalité nécessite souvent une collaboration entre services de police, au pays et à l'étranger.

Les criminels ne se soucient pas d'obtenir des autorisations judiciaires et d'agir dans les limites de la loi. Ils ne sont pas non plus assujettis aux contraintes de ressources qui limitent le rayon d'action de la police.

« Il s'agit d'un cadre de compétence extraterritoriale : la preuve ou le criminel peuvent se situer dans un pays différent; un criminel canadien peut cibler un autre pays, précise le s.é.-m. Rosa. Nous sommes souvent appelés à collaborer avec nos partenaires aux enquêtes ou à l'échange d'information. »

La GRC met en œuvre une démarche axée sur les renseignements, y compris ceux recueillis par les partenaires canadiens et étrangers. Dans la présente affaire, le suspect a attiré l'attention d'un partenaire policier, qui a relayé l'information à la GRC.

À l'issue de trois mois d'enquête sur le suspect, l'EEC possédait assez de preuves pour soumettre à un juge des motifs raisonnables d'obtenir et d'exécuter un mandat de perquisition.

PASSAGE À L'ACTION

Armée du mandat, l'équipe est prête à passer à l'action. Si l'EEC est basée à Ottawa, les

Une fois obtenu un mandat de perquisition, l'Équipe d'enquête sur la cybercriminalité peut saisir les preuves nécessaires.

Serge Gouin, GRC

crimes sur lesquels elle enquête peuvent avoir lieu n'importe où au pays.

« Je me demande ce que va penser le suspect lorsque nous frapperons à sa porte demain », avoue le gend. Veilleux.

Il reste encore bien des détails à régler lorsque l'équipe se rendra à destination, notamment la façon d'entrer dans la résidence.

Malgré toute la planification du monde, certains éléments demeurent incertains. Par exemple, on ne sait pas si le suspect sera chez lui, car il ne fait pas actuellement l'objet de surveillance.

« Il doit être à la maison, précise le gend. Veilleux. Il dort toujours chez lui... S'il n'y est pas, nous ferons quand même la perquisition. »

Lorsque toute l'équipe est arrivée à l'hôtel, on tient une nouvelle séance. Les dix membres de la GRC et quelques membres de services partenaires se retrouvent dans une petite chambre.

On confirme le déroulement de l'opération : cogner et attendre que le suspect ouvre, et n'entrer de force qu'au besoin.

« Il faudra faire preuve de souplesse, explique le gend. Veilleux. Je peux concevoir toute une série de scénarios, mais il faudra aller avec le flot des événements. À demain! »

LA DESCENTE

Après tout ce travail, voici venu le moment décisif. L'opération est le point culminant de la persévérance, de recherches méticuleuses et de l'application de bonnes techniques d'enquête.

« Recueillir des éléments de preuve concrets dans ce genre d'enquête est particulièrement difficile, explique le s.é.-m. Rosa. Il ne suffit pas d'exécuter spontanément un mandat de perquisition au hasard. Il faut parvenir au seuil de preuve, ce qui peut être très ardu. »

L'équipe s'est réunie dans un stationnement à quelques minutes des lieux. La plupart des membres sont en civil, avec leur gilet pare balles et leur arme sous leur veston. Seul signe évident qu'il s'agit de policiers : les deux membres en uniforme les accompagnant.

Après un dernier conciliabule, les membres montent en voiture pour se rendre à la résidence du suspect.

Les deux analystes en expertise judiciaire numérique, des civils, suivent. Ils n'entreront dans le logis qu'une fois le suspect arrêté et les lieux sécurisés.

Serge Gouin, GRC

Les membres de l'Équipe d'enquête sur la cybercriminalité revoient le plan d'attaque une dernière fois avant d'exécuter un mandat de perquisition.

« En général, nous sommes les derniers entrés et les derniers sortis », souligne un analyste au GCT. Officiellement, il fait partie de l'équipe d'expertise judiciaire numérique, mais il arrive que les membres des deux groupes intervertissent leurs rôles.

À mesure qu'on relève des ordinateurs, des cellulaires, des clés USB, voire des CD gravés, les enquêteurs et analystes en expertise judiciaire numérique traiteront les données sur place afin de déterminer ce qui doit être saisi.

Ce traitement permettra de gagner du temps plus tard, car tout ce qui est saisi doit répondre aux critères du mandat, et la GRC en assume la responsabilité.

Près d'une heure plus tard, M. Grondin et son partenaire reçoivent le signal : le suspect est appréhendé. C'est l'éventualité la plus souhaitable – tout s'est déroulé sans pépin.

Le suspect est mis en détention et amené au détachement local de la GRC. Il sera interrogé par la suite.

L'enquêteur chargé de l'interrogatoire, le gend. Poulin, a une stratégie en tête.

« J'ai vérifié les éléments de preuve recueillis contre le suspect, explique-t-il. Tout agent interrogateur, peu importe le dossier, doit autant que possible faire ses recherches au préalable. Si on connaît les intérêts et les antécédents du suspect, on peut les mettre à profit. Dans le présent cas, nous avions beaucoup de renseignements sur le suspect. »

Assis en face du suspect, le gend. Poulin applique son plan. Dans les heures qui suivent, il engage un dialogue avec l'homme. Puis il commence à l'interroger sommairement sur ses activités.

Le gend. Poulin prend appui sur chaque réponse, intensifiant la pression, puis la relâchant au besoin pour maintenir le fil de la conversation.

En fin de compte, la stratégie a fonctionné : il a obtenu des aveux.

Au logis du suspect, la perquisition s'est bien déroulée. On ne s'est buté sur aucun obstacle numérique et on a pu recueillir les éléments voulus.

Cette journée a été longue, mais fructueuse.

SUR LA BONNE VOIE

Le serg. Beaulieu est satisfait de son équipe et des résultats de son opération soigneusement menées.

« Les résultats obtenus dépassent nos attentes, constate-t-il. Nous voulions repérer le crime et faire enquête; si tout va bien, nous aurons identifié et traduit le malfaiteur en justice. Nous y sommes presque. » ■

**Certains noms ont été omis pour des raisons de sécurité.*

Serge Gouin, GRC

Le cap. Darren Birnie applique la technique de la programmation *in situ* pour acquérir le contenu complet de la mémoire d'un appareil numérique tout en laissant les données originales intactes.

DERRIÈRE L'ÉCRAN

DÉCOUVERTE ET INTERPRÉTATION DE DONNÉES PAR LES EXPERTS EN CRIMINALISTIQUE NUMÉRIQUE

par Deidre Seiden

Dans les bureaux ottaviens du Groupe de la criminalité technologique (GCT) de la GRC, à la Division nationale, une simple demande d'ouverture de clé USB a tourné en une discussion animée sur la bonne procédure à suivre.

Une part essentielle du travail des experts en criminalistique numérique consiste à préserver l'intégrité des données qui se trouvent sur les dispositifs saisis. Il leur est absolument nécessaire de connaître tous les faits avant de tenter d'accéder aux données. Alors quand un collègue d'un autre service vient leur demander d'examiner le contenu d'une clé USB, ils ont des questions.

Qu'est-ce que c'est? D'où cela provient-il? Le simple fait d'ouvrir les fichiers peut avoir des conséquences fâcheuses.

« On doit faire une copie-image de la clé USB pour en préserver le contenu original, explique le serg. David Connors, s.-off.resp. des activités de l'équipe de criminalistique numérique du GCT. Pour introduire un élément de preuve devant le tribunal, il faut démontrer qu'il s'agit de l'élément même qui a été trouvé sur les lieux du crime, ce qui n'est bien sûr pas possible lorsque, pendant plus d'un an, tout le monde et son voisin a eu l'occasion d'y toucher. Chaque fois qu'on touche à un dispositif, on en prend note. »

En plus de préserver la preuve, les experts en criminalistique numérique mènent une enquête structurée en recueillant, en classant et en validant les informations numériques trouvées afin de reconstituer des événements passés. Il s'agit pour eux, en gros, de rendre l'élément de preuve intelligible pour quelqu'un qui n'a pas de formation en haute technologie.

DONNÉES NUMÉRIQUES

On voit tout de suite pourquoi les analystes et enquêteurs de criminalistique numérique (ECN) sont perçus par leurs clients comme des mordus de l'informatique : la quantité d'ordinateurs, de téléphones cellulaires, de réseaux informatiques et d'autres appareils qui composent leur environnement de travail donnerait le vertige à n'importe qui.

« C'est un travail difficile, déclare le cap. Darren Birnie, ECN au sein du GCT. Mais c'est très stimulant quand on aime l'apprentissage continu et les défis toujours nouveaux. J'ai commencé en 2009, et encore aujourd'hui, je continue à avoir des surprises quand j'examine des systèmes. »

Cette évolution est en partie dictée par la rapidité des progrès technologiques.

« On doit constamment s'adapter, observe, un analyste civil au sein du GCT. Tous les deux ou trois mois, un nouveau cellulaire apparaît sur le marché. Un jour, on fait telle chose d'une certaine façon, et le lendemain, d'une autre façon. On est toujours en train de faire des recherches pour être à la page. »

Le GCT a beau veiller à rester continuellement à jour, les enquêtes, elles, prennent du temps. Le GCT à Ottawa a participé à l'enquête portant sur l'attaque au virus Heartbleed lancée contre l'Agence du revenu du Canada, en 2014. Le 6 mai 2016, Stephen Solis-Reyes a plaidé coupable à deux chefs d'accusation de méfait volontaire (données), à une accusation d'utilisation non autorisée d'un ordinateur et à une accusation d'entrave à un agent de la paix.

Ces derniers mois, le cap. Sébastien Laurendeau, ECN au sein de l'équipe d'enquête en cybercriminalité (EEC) qui est intégrée au GCT, a passé ses journées à fouiller des données sur disque dur à la recherche d'éléments de preuve pouvant relier un suspect à une infraction. Au dire du cap. Laurendeau, ce travail procure de la satisfaction, même s'il exige de la patience.

« Arriver à faire des liens, c'est gratifiant, affirme le cap. Laurendeau. Le simple fait de découvrir comment un délinquant s'y est pris pour commettre une infraction est une source de plaisir, tout comme le simple fait de constater qu'on avance au lieu de piétiner. »

APPRENTISSAGE DU MÉTIER

Le cap. Laurendeau n'était pas un mordu de technologie avant de se joindre à l'EEC. Son

intérêt est né au cours d'une affaire de leurre en ligne à laquelle il a travaillé lorsqu'il était affecté aux services généraux au Nouveau-Brunswick. Il avait alors demandé conseil au GCT de sa division.

« Avec l'aide des fournisseurs de services, j'ai pu, à partir des adresses IP, retrouver la trace du suspect. Ce travail m'a vraiment allumé, raconte le cap. Laurendeau. Les gens croient bénéficier de l'anonymat quand ils sont en ligne, mais ils se trompent. J'ai fini par trouver mon suspect, je l'ai arrêté, puis il a été jugé et condamné. »

Cette expérience l'a conduit à poursuivre sa carrière en criminalistique numérique. Il a suivi quelques cours pour élargir ses connaissances, puis a postulé. Il a fait partie du GCT du Nouveau-Brunswick avant d'intégrer l'EEC à Ottawa.

Plusieurs des membres du GCT ont des connaissances en informatique, mais ce n'est pas requis. Aux candidats retenus est offert un programme de formation pratique qui combine mentorat en contexte de travail et cours d'informatique judiciaire au Collège canadien de police.

D'ordinaire, l'employé a besoin d'un an ou deux pour devenir un ECN autonome, ce qui veut dire qu'un long laps de temps s'écoule entre son embauche et le moment où il peut commencer à travailler de façon indépendante.

DOMAINE EN EXPANSION

À en juger par les outils et l'équipement de pointe dont l'équipe dispose, par exemple la salle de serveur de plusieurs millions de dollars qui fournit une protection contre les attaques informatiques, il est évident que le GCT est une priorité pour la GRC.

Chaque province est dotée d'un GCT appelé à soutenir les détachements locaux. Ces groupes provinciaux ont le plus souvent affaire à des crimes de rue (p. ex. voies de fait, entrée par effraction, vol, fraude, querelles de ménage), mais il leur arrive aussi de participer à des enquêtes majeures (p. ex. homicide, fraude à grande échelle, trafic de drogue, crime organisé, criminalité aux frontières et aux douanes, sécurité nationale).

Le GCT d'Ottawa se distingue en ceci qu'il contribue surtout aux affaires de grande envergure et de longue haleine dont sont chargées les Enquêtes internationales et délicates de la Division nationale, qui s'occupent des dossiers de nature politique et des cas de corruption, d'abus de confiance, de crime de guerre et d'enlèvement. Le GCT d'Ottawa soutient également les services de sécurité routière de la RCN, les services généraux de la Police de protection, les Services de PDM ainsi que le Peloton de protection du premier ministre et celui du gouverneur général. Et comme le GCT d'Ottawa est intégré à l'EEC, il travaille aussi à élucider des cybercrimes.

Aujourd'hui, presque toutes les enquêtes comportent un élément de criminalistique numérique. « En réalité, chaque affaire peut receler un aspect numérique, analyse le cap. Birnie. Mais c'est aussi une réalité que les ressources sont rares, de sorte qu'il faut faire le tri entre ce qui mérite qu'on y consacre du temps et ce qui peut être négligé sans nuire à la poursuite et à ses chances de succès. Il n'y a tout simplement pas assez de technologues judiciaires. »

D'après le serg. Connors, cela signifie qu'il demeure nécessaire de former des employés en criminalistique numérique et de fournir au personnel de première ligne l'information dont il a besoin.

« À mesure qu'augmente le nombre de gens qui règlent leurs affaires quotidiennes dans le monde virtuel, de plus en plus de criminels cherchent à pénétrer dans cet espace et, par conséquent, de plus en plus d'opérations policières y sont menées », conclut le serg. Connors. ■

**Certains noms ont été omis pour des raisons de sécurité.*

LABORATOIRE MOBILE

par Amelia Thatcher

Le Groupe de la criminalité technologique (GCT) de la GRC en Nouvelle-Écosse transporte son expertise directement sur les lieux de crime grâce à un labo mobile unique. La remorque blanche, sans marquage, accompagne les policiers lorsqu'ils exécutent des mandats de perquisition.

« Sur les lieux d'une perquisition, nous sommes à la merci de l'environnement dans lequel nous nous trouvons, dit le cap. Duane Flynn, analyste judiciaire du GCT. Le labo mobile est un endroit sécuritaire où travailler. »

Depuis trois ans, le labo mobile offre un lieu de travail propre et sécuritaire aux analystes du GCT. Il est doté d'un générateur, d'un petit bureau où deux analystes peuvent s'asseoir et d'un autre banc pour deux enquêteurs.

« Nous pouvons aller sur place, extraire des données et les fournir immédiatement aux enquêteurs, dit le serg. Royce MacRae, responsable du GCT. Non seulement on gagne du temps, mais on offre aux enquêteurs un bien meilleur produit. Lorsqu'ils quittent le lieu, ils ont des pistes pour interroger les suspects. »

Avant de commencer, les analystes du GCT discutent de ce qu'ils doivent chercher avec l'enquêteur chargé de l'affaire. Ils essaient de savoir à l'avance à quels types d'appareils ils auront affaire – ordinateur, tablette, téléphone intelligent ou autre. Le cap. Flynn dit que son équipe passe environ cinq heures à examiner des données numériques sur les lieux.

« Notre but est de déterminer les types d'appareils qui feront avancer l'enquête, dit-il. Parfois, c'est une aiguille dans une botte de foin vu la quantité de données que nous trouvons, mais nous essayons d'en éliminer le plus possible. »

Cpnd. Todd Bromley, CBC

Des membres du GCT (N.-É.) analysent des appareils électroniques sur les lieux dans leur labo mobile pendant que la police exécute des mandats de perquisition.

QUEL EST LE PLUS GRAND DÉFI DE LA POLICE EN MATIÈRE DE CYBERCRIMINALITÉ?

LES SPÉCIALISTES :

- **Jeffrey Thomson, analyste de renseignements criminels, Centre antifraude du Canada, North Bay (Ont.)**
- **Surint. pr. Jeff Adam, Directeur général des Services d'enquêtes techniques, Ottawa, GRC**
- **Bessie Pang, directrice administrative, The Society of the Policing of Cyberspace (POLCYB), Richmond (C.-B.)**

JEFFREY THOMSON

La cybercriminalité n'a rien de nouveau. Pourtant, aujourd'hui encore, on entend des choses comme « y a peu de chances de pouvoir faire une arrestation », « on n'extradera pas vers le Canada », « c'est en dehors de notre territoire de compétence », « la preuve est à l'étranger » ou « les ressources nous manquent ». Ces commentaires reflètent-ils fidèlement notre connaissance de la cybercriminalité et notre capacité à enquêter? Ou s'agit-il d'autre chose?

Malgré l'article 7 du *Code criminel*, qui autorise les tribunaux canadiens à connaître de certaines infractions comme si elles avaient été commises au pays, d'aucuns estiment que la législation canadienne ne permet pas de faire enquête sur les infractions extraterritoriales.

Ces difficultés ne datent pas d'hier. Des études et évaluations relatives à la cybercriminalité réalisées entre 2007 et 2009 nous avertissaient que l'expansion mondiale des usages d'Internet s'accompagnerait d'une hausse de la cybercriminalité, et elles prédisaient que les nouvelles technologies, les logiciels, les maliciels, la sécurité des systèmes informatiques, l'anonymat et les questions de compétence légale poseraient des difficultés à la police, qui aurait besoin de plus de ressources pour enquêter sur ce genre d'affaires. Or voici que, près de dix ans plus tard, nous sommes toujours aux prises avec les mêmes enjeux.

Quel est le nœud du problème? Pour beaucoup de corps de police, c'est une question d'effectif et de connaissances. Les policiers qui font face à un cas de « rançongiciel » ou d'intrusion dans des courriels d'affaires sont censés enquêter et recueillir des déclarations et des preuves alors que, bien souvent, ils n'ont jamais traité ce genre d'infraction et n'y comprennent pas grand-chose.

Même lorsqu'ils ont pu monter un dossier solide, beaucoup sont réduits à se demander « et maintenant, qu'est-ce qu'on fait? » parce que, par exemple, l'argent a été envoyé à l'étranger, les courriels ou les faux sites Web sont hébergés à l'étranger, la drogue saisie a été achetée sur le Web invisible ou les malfaiteurs se trouvent dans un autre pays.

La police canadienne a-t-elle les outils et les pouvoirs qu'il faut pour traquer les contrevenants? Et aurait-elle l'appui du système de justice pénale, qui est déjà surchargé, qui est lui aussi mal équipé pour régler les affaires de cybercriminalité et que beaucoup de policiers jugent trop indulgent envers les fraudeurs en ligne et autres cybercriminels.

En 2014, le gouvernement canadien a édicté la *Loi sur la protection des Canadiens contre la cybercriminalité*. Cette loi, qui selon certains sert à incorporer au droit canadien les obligations stipulées dans la Convention de Budapest sur la cybercriminalité (2001), a été adoptée pour accroître les pouvoirs d'enquête de la police relativement aux activités en ligne. Mais qu'en est-il résulté? Est-ce la majorité des policiers qui connaissent et comprennent la nouvelle loi?

La question à poser n'est donc peut-être pas tant celle de savoir quel est le plus grand défi que la cybercriminalité lance à la police que celle de savoir pourquoi la cybercriminalité est devenue si difficile à réprimer. La réponse type à la première question évoque

la mise en place, à chaque niveau du travail policier, d'activités de formation, de ressources et de capacités, y compris les connaissances. Quant à la seconde question, elle nous invite à repérer les secteurs à améliorer où de modestes investissements suffiraient à combler les lacunes actuelles du renseignement.

SURINT. PR. ADAM

Les principes de police formulés par sir Robert Peel en 1829 datent d'une époque où la victime, le contrevenant et les autorités policières et judiciaires se trouvaient tous au même lieu. Le premier principe – prévenir la criminalité et le désordre – reposait sur le caractère local du crime et sur l'aptitude de la police à remplir sa mission de faire respecter la loi et l'ordre.

Vous voyez où je veux en venir. Le mandat officiel de la police, qui consiste à maintenir l'ordre, à prévenir la criminalité, à recueillir des preuves, à arrêter les délinquants et à les traduire en justice, est mis à rude épreuve par les réalités du monde globalisé d'aujourd'hui. Le contrevenant se trouve presque toujours dans un autre pays; or les frontières géopolitiques, qui ont durant des siècles servi l'intérêt des nations, sont sans objet dans le cyberespace. Et accorder la primauté au respect de ces frontières revient à nier l'utilité d'Internet pour le commerce, l'éducation et les échanges culturels internationaux.

La culture policière canadienne a pris forme au fil du temps : prévenir le crime, maintenir l'ordre, recueillir des preuves et livrer l'accusé à la justice. L'essentiel de nos ressources a été employé à produire les livrables liés à ces fonctions, et c'est dans les deux dernières de la liste qu'il est le plus facile de mesurer les résultats obtenus. Il est beaucoup plus aisé de faire rapport sur les infractions, les arrestations, les déclarations de culpabilité et les acquittements que de rendre compte du nombre de crimes prévenus ou de l'aide qui a été apportée aux victimes.

Mais dans le cyberespace, il est nettement plus difficile d'arrêter les coupables et de les traduire en justice. Si la police est incapable d'attraper les délinquants, d'autant plus d'efforts doivent être consacrés à la prévention et à l'aide aux victimes, d'où cette question : la police est-elle la mieux placée pour remplir ces fonctions? Je crois qu'il faut, pour y répondre, adopter une perspective embrassant toute la société, car la façon traditionnelle et éprouvée de s'attaquer au crime ne peut être efficace dans le cyberespace. La police ne résoudra pas ce problème toute seule.

D'autres difficultés entravent les enquêtes sur les cybercrimes. Où est la preuve? Lorsqu'un pirate informatique accède à des données stockées dans le nuage, où l'infraction a-t-elle lieu? Et qui a compétence pour enquêter?

Internet a complètement bouleversé notre quotidien et notre façon d'échanger les uns avec les autres. C'est en travaillant ensemble à relever les défis que présente la cybercriminalité que nous pourrons amener les citoyens à faire la police dans le cyberespace à la place des policiers.

BESSIE PANG

Dans le monde branché d'aujourd'hui, le grand écheveau de l'Internet des objets (IdO) perfuse tous les aspects de la vie quotidienne, du frigo ou thermostat intelligent au matelas intelligent qui s'ajuste pour maximiser le confort du dormeur. D'après un rapport de Berg Insight, l'Europe et l'Amérique du Nord comptaient en 2015 17,9 millions de « maisons intelligentes ». D'ici 2020, l'Amérique du Nord en comptera 46,2 millions, soit 35 p. 100 de l'ensemble des foyers.

Le consommateur est constamment poussé à monter à bord du train rapide des outils intelligents. Prompt à adopter divers appareils intelligents à la maison ou au travail pour simplifier ses tâches quotidiennes, il est souvent peu vigilant à l'égard des vulnérabilités techniques qui pourraient prêter le flanc à l'attaque d'un cybercriminel ou d'un pirate informatique.

En général, au moment de faire un achat qui touche à l'IdO, le consommateur ne cherche pas à savoir si l'objet intelligent de son choix accepte les correctifs – or c'est justement là le genre de questions qu'il devrait poser quand il se renseigne sur des produits.

Le risque d'être victime d'un cybercrime est plus élevé chez certains groupes sociaux comme les aînés, les immigrants et les réfugiés en raison des barrières physique, sociale, linguistique et culturelle qui les séparent des sources d'information sur la cybercriminalité. Par exemple, un aîné à mobilité réduite peut maintenant recourir à divers dispositifs médicaux lui permettant de conserver son autonomie, certains transmettant des données en temps réel au médecin traitant, d'autres avisant un proche aidant par texto, courriel ou téléphone chaque fois que l'aîné saute un repas. Il existe même un vêtement intelligent qui active des coussins gonflables lors d'une chute.

Attiré par les avantages évidents du dispositif médical intelligent, le patient n'a probablement pas demandé au médecin en quoi un accès illicite au dispositif risquait de mettre sa santé en péril, surtout dans une situation d'urgence.

Amener les consommateurs à prendre des décisions éclairées après avoir soupesé les risques et avantages que présentent les produits touchant à l'IdO peut s'avérer salutaire dans les cas où l'appareil intelligent cesse de fournir des solutions intelligentes.

POLCYB est un organisme international à but non lucratif qui vise à accroître la collaboration public-privé en vue de faciliter la diffusion d'informations relatives aux politiques, aux stratégies et aux pratiques exemplaires de prévention, de détection et de répression de la cybercriminalité.

POLCYB s'emploie en outre à sensibiliser la population à l'égard de la cybercriminalité. Pour POLCYB, le principal défi consiste à faciliter l'accès du public à l'information disponible sur la vulnérabilité de l'IdO eu égard aux crimes informatiques. Il est donc essentiel d'élaborer des stratégies de sensibilisation qui intègrent des modes efficaces de prestation de services.

En plus de promouvoir l'action de partenariats public-privé dans l'éducation du public, il est crucial d'obtenir la collaboration d'organismes communautaires. On pourrait inciter ceux-ci, qu'il s'agisse de services de counselling, de services de réinstallation des immigrants, de résidences-services ou de centres communautaires, à collaborer avec les organismes d'application de la loi et leurs partenaires de l'industrie en vue de transmettre l'information visant à prévenir la cybercriminalité sous une forme adaptée à leur clientèle respective. Une fois le prestataire de services dûment formé à prévenir la cybercriminalité, il peut agir comme foyer d'information et instruire ses clients de manière informelle.

L'éducation du public est un aspect important de la prévention de la cybercriminalité, mais les organismes d'application de la loi ont besoin du soutien des groupes communautaires. Et à mesure que l'IdO pénétrera dans tous les secteurs de la société, il deviendra de plus en plus impératif de favoriser le développement continu des capacités communautaires. ■

CONTAMINATION D'INTERNET

PIRATES ET RÉSEAUX ZOMBIES DANS LA MIRE DU CYBERRENSEIGNEMENT

par Amelia Thatcher

L'Internet est devenu indispensable au quotidien – qu'il s'agisse de régler une facture, de commander un repas ou de trouver l'âme sœur. Son utilisation a décuplé, tout comme son exploitation malveillante par les criminels.

« La cybercriminalité ne connaît pas de frontière, peu importe le domaine et le champ d'activité, explique la surint. Marie-Claude Arsenault, off. resp. de la cyberéquipe du Centre national de coordination du renseignement (CNCR) de la GRC. La plupart des délits, qu'ils soient facilités par le Web ou qu'ils ciblent celui-ci, comportent une dimension technologique ou numérique. »

Pour suivre le rythme de cette migration rapide de la société vers le Web, le CNCR a créé en 2014 l'équipe de cyberrenseignement de la surint. Arsenault dans le cadre de la stratégie de lutte contre la cybercriminalité de la GRC. Son mandat : recueillir des données afin de cibler les enjeux d'application de la loi pour les enquêteurs provinciaux, nationaux et à l'étranger.

« Nous nous efforçons de relever des pistes et de monter un dossier; ainsi, lorsqu'une affaire est confiée à une division (province ou territoire), ses membres peuvent l'aborder sur le champ, précise la surint. Arsenault. Débordés, ils n'ont pas toujours le loisir d'étudier le prochain dossier. Notre rôle consiste à faire les recherches préliminaires afin de leur simplifier la tâche. »

Si la plupart des enquêtes ont une composante technologique, l'équipe de la surint. Arsenault se limite à un aspect précis de la criminalité en ligne : les stratagèmes qui ciblent la technologie en tant que telle.

« Nous nous concentrons sur deux articles du *Code criminel* : les méfaits à l'égard de données informatiques et l'utilisation non autorisée d'un ordinateur, c.-à-d. le piratage, explique le s.é.-m. Paul Poloz, responsable des priorités du renseignement au CNCR. Pour d'autres crimes comme la fraude, l'exploitation d'enfants et le piratage de courriels, l'ordinateur, la technologie ne constituent pas une fin, mais un moyen. Nous nous consacrons strictement aux activités de cybercriminalité. »

L'équipe cible les pirates qui créent ou utilisent un logiciel malveillant (dit maliciel) par exemple sous forme de virus informatique. Elle relève la piste numérique de ces cybercriminels, à la recherche de tous ceux qui compromettent l'infrastructure d'Internet.

RÉSEAUX ZOMBIES

Une des plus grandes menaces contre Internet – et l'une des priorités de l'équipe – sont les réseaux zombies – tout ensemble de machines reliées à Internet qui sont compromises et contrôlées pour exécuter des tâches inhabituelles, généralement à des fins malveillantes, criminelles.

Une machine est compromise lorsqu'un maliciel s'infiltre dans le système sans le consentement de son propriétaire. La machine infectée tombe sous le contrôle à distance du cybercriminel.

En créant un réseau zombie, le pirate cherche à contaminer non pas une ou deux machines, mais des centaines d'ordinateurs, de téléphones intelligents, de systèmes GPS, de routeurs et tout autre élément connecté à Internet. Il peut commander au réseau zombie de transmettre des pourriels et des virus, entre autres actes cybercriminels.

« Caméras, systèmes de sécurité domiciliaire, même les réfrigérateurs qui sont reliés à Internet – tous sont vulnérables, explique Greg Simmonds, gestionnaire de l'équipe de cyberrenseignement du CNCR. Nous tenons ces éléments pour acquis, mais un pirate futé qui sait comment en prendre le contrôle peut s'en servir comme porte d'accès pour commettre des actes criminels. »

Parmi ces délits, citons le déni de service distribué. Dans la plupart de ces attaques, le pirate commande au réseau zombie de submerger de trafic un site Web, de façon à le faire planter, que ce soit aux fins de chantage, de concurrence ou simplement pour exprimer sa colère contre le propriétaire du site.

« Les victimes, les malfaiteurs et les serveurs peuvent se trouver dans des pays distincts, explique la surint. Arsenault, d'où la difficulté d'appliquer la loi. Pour lutter contre la cybercriminalité, il est donc important d'établir une coopération internationale. »

POUR RESTER À L'AVANT-PLAN

Selon la surint. Arsenault, il faut d'abord démystifier le monde de la cybercriminalité si l'on veut réussir à endiguer ces activités illicites en ligne.

« La police est intimidée par la situation, souligne-t-elle. Face à 20 introductions par effraction, elle sait intervenir. Mais devant 20 cyberattaques, elle ne bronche pas, ne considérant pas toujours qu'il s'agit d'un crime. »

La surint. Arsenault dit espérer que son œuvre de sensibilisation changera les choses, pour les équipes spécialisées et les membres sur le terrain. Et si la plupart des services de police ont du rattrapage à faire en matière d'enquête, sous un aspect en particulier, la GRC est à l'avant-plan.

« En matière de renseignement, nous avons une longueur d'avance, explique-t-elle. Peu de corps policiers peuvent se targuer d'avoir une équipe spécialisée en cyberrenseignement. » ■

Amelia Thatcher, GRC

En avril dernier, la surint. Marie-Claude Arsenault, de la GRC, ainsi que des représentants de services de police étrangers ont échangé des pratiques exemplaires lors du sommet international de lutte contre la cybercriminalité.

APTITUDES EN CYBERRENSEIGNEMENT

DÉVELOPPÉES AU COLLÉGE CANADIAN DE POLICE

par Amelia Thatcher

Dans Internet, les criminels agissent dans l'anonymat, ce qui complique les cyberenquêtes policières. Pour maintenir une longueur d'avance sur les criminels, le Collège canadien de police (CCP) à Ottawa a ajouté un nouveau cours à son programme : le Cours d'enquêteur sur la cybercriminalité (CEC).

Inauguré en 2016, le cours de dix jours inculque les aptitudes nécessaires pour mener une cyberenquête approfondie. On y aborde les cas où la technologie est ciblée, comme l'utilisation non autorisée d'un ordinateur, les méfaits à l'égard de données informatiques et le piratage.

« En acquérant une idée générale des concepts et des technologies en cause dans leur enquête, les policiers peuvent déterminer ce qu'il faut saisir et conserver, et comprendre les cas où il faut agir rapidement », explique le serg. Nicolas Bernier, instructeur principal en cybercriminalité au CCP.

Le gend. Scott Noseworthy, enquêteur à la GRC en Alberta, a suivi le cours plus tôt cette année. Il estime avoir acquis une information précieuse qui l'a aidé à résoudre une affaire de rançongiciel – un programme malveillant qui bloque l'accès à un système jusqu'au versement d'une somme d'argent.

« Après avoir suivi le cours, nous avons été saisis d'un cas important de la part du responsable d'une infrastructure essentielle, et nous avons pu intervenir avec efficacité, précise-t-il. Conscients des ressources disponibles, nous avons coopéré avec d'autres services de police de façon à favoriser le dénouement de l'enquête et à mieux assister les victimes. »

FAMILIARISATION AVEC LA TECHNOLOGIE

Les activités cybercriminelles sont en hausse au pays, selon les derniers chiffres de la GRC. En 2013, celle-ci a recensé environ 4 400 incidents, soit 40 p. 100 de plus que les 1 300 cas signalés en 2011. Cette montée de la cybercriminalité a incité le CCP à actualiser ses cours et à en créer de nouveaux à l'intention des policiers étrangers et des partenaires fédéraux.Le CEC est le dernier en date offert par l'Institut d'apprentissage en criminalité technologique au CCP. L'Institut offre 14 cours dans un éventail de domaines (expertise judiciaire numérique, technologie et cybercriminalité) pour les agents de la GRC et d'autres services de police, ainsi que les employés civils assumant des fonctions de renseignement ou d'enquête.

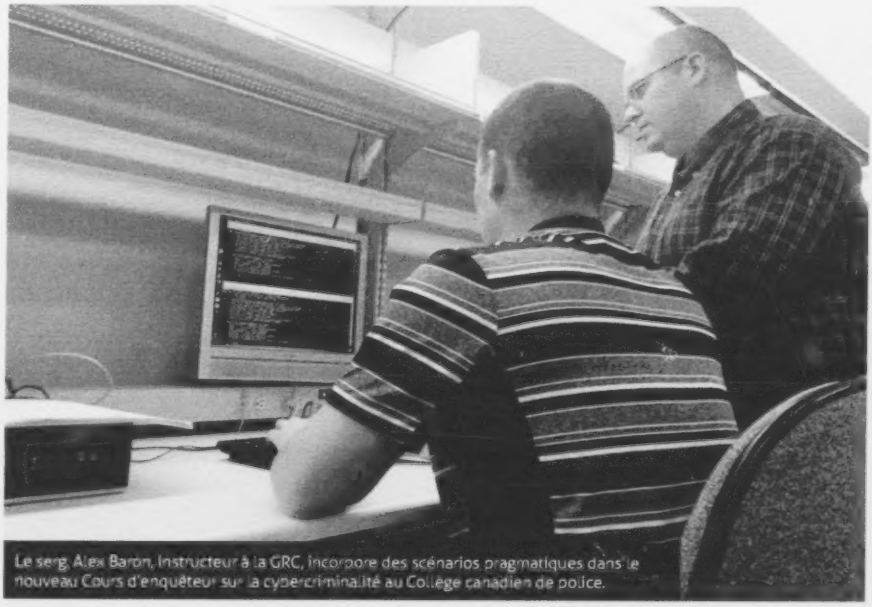


Photo fournie par le serg. Alex Baron, GRC

Le serg. Alex Baron, instructeur à la GRC, incorpore des scénarios pragmatiques dans le nouveau Cours d'enquêteur sur la cybercriminalité au Collège canadien de police.

Ces différents programmes, cours et ateliers offrent deux champs de spécialisation : le premier pour les enquêteurs cherchant à raffiner leurs méthodes d'enquête sur les crimes dans Internet, et le second pour ceux désirant se spécialiser dans l'expertise judiciaire numérique, ou l'analyse et l'extraction de données d'appareils numériques. Chaque cours couvre également les notions d'application de la loi à l'ère de la technologie.

« Si certaines notions traditionnelles de perquisition et de saisie s'appliquent, nombre de cas mettent en cause de nouvelles technologies, souligne le serg. Bernier. Il importe pour les membres de savoir immédiatement l'orientation à donner à leur enquête, car les preuves peuvent être éphémères – et disparaître à jamais si on ne les relève pas sur-le-champ. »

POUR UNE INTERVENTION EFFICACE

Le CEC est enseigné par le serg. Alex Baron, instructeur principal en cybercriminalité à la GRC. Il est appuyé par quelque 20 spécialistes, dont des représentants du FBI.

« Le cours est l'occasion de nouer des contacts très importants dans le cyberespace, précise-t-il. Il faut unir nos forces afin d'élaborer un mode d'opération commun et concerté. »

Le serg. Baron et les autres experts offrent aux participants des scénarios pragmatiques qui leur permettent de recueillir de l'information ensemble. Dans de nombreux cas, les pirates laissent une piste numérique; le serg. Baron apprend aux enquêteurs à relever cette piste et à poser les bonnes questions pour résoudre l'affaire.

Depuis le cours, le serg. Noseworthy a travaillé à plusieurs dossiers et il confirme la valeur de mieux connaitre les subtilités d'Internet et de la technologie en cause.

« Le cours nous enhardit à aborder les enquêtes cybercriminelles et nous donne les outils pour affronter non seulement les crimes banals comme la fraude de 200 $ contre grand-mère, dit-il, mais aussi les cas d'envergure ciblant les grandes entreprises et les infrastructures essentielles à l'échelle du pays; le policier doit désormais être rompu à ce genre d'enquête. » ■

EN QUÊTE D'ÉLÉMENTS DE PREUVE CONCRETS

DES NON-SPÉCIALISTES FORMÉS AU TRIAGE DES APPAREILS NUMÉRIQUES

par Deidre Seiden

Kathleen Vilac, membre civile de l'Équipe intégrée d'enquête sur les homicides (EIEH) de la GRC en C.-B., se remémore l'un des premiers cas auquel elle a collaboré dans le cadre du programme de triage des éléments de preuve numérique (TEPN).

On était en 2012, et il s'agissait d'une affaire de nourrisson secoué. M^me^ Vilac s'était vu confier un ordinateur saisi par l'EIEH pour y rechercher des éléments de preuve.

Dans le passé, de telles pièces à conviction auraient été transmises directement à un spécialiste de l'expertise judiciaire numérique du Groupe de la criminalité technologique (GCT) de la province. À ses débuts, le groupe avait communiqué avec les équipes d'enquête pour leur dire qu'il pouvait les aider à saisir et à traiter les éléments de preuve numérique.

« À l'époque, nous avions moins de travail que les enquêteurs, précise le s.é.-m. Clint Baker, s.-off. des opérations du GCT en C.-B. Désormais, c'est l'inverse qui est vrai. Peu importe le genre d'enquête, celle-ci implique probablement des éléments de preuve numérique. »

Avec la propagation fulgurante des cellulaires et des ordinateurs, pratiquement tous les appareils saisis sont transmis au GCT, qu'ils renferment des éléments de preuve ou non. Le groupe est donc débordé et connait un arriéré.

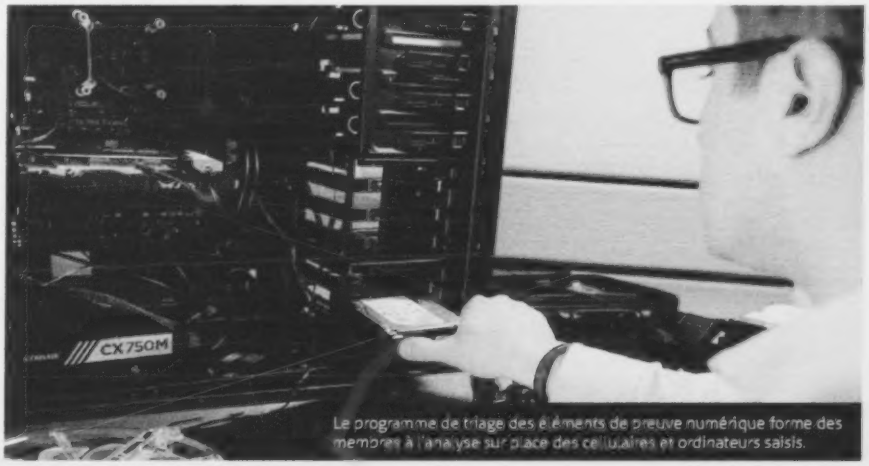
« Quelle utilité pour l'enquêteur de nous envoyer un appareil s'il doit attendre deux ans pour obtenir des éléments de preuve concrets?, explique le s.é.-m. Baker. Nous devons servir les enquêteurs. »

UNE NOUVELLE FAÇON DE FAIRE

Pour alléger l'arriéré, les membres du GCT ont créé le programme de TEPN en 2009.

L'idée était novatrice dans le secteur de la criminalité technologique. Jusque-là, seuls les spécialistes de l'expertise judiciaire numérique étaient habilités à faire de l'analyse.

« Nous devions aplanir cet obstacle, explique le serg. Ben Hitchcock, qui a participé à l'élaboration du programme. Les membres affectés au TEPN n'effectuent pas d'analyse. Ils se chargent d'extraire des données et de produire un rapport d'observation. Une distinction très importante. »



Le programme de triage des éléments de preuve numérique forme des membres à l'analyse sur place des cellulaires et ordinateurs saisis.

Serge Gouin, GRC

Les membres du TEPN font état de leurs observations. « N'importe qui peut constater l'existence d'une image d'exploitation d'enfant dans un ordinateur, souligne-t-il. Mais on ne peut pas retracer nécessairement l'origine de l'image, comment elle s'est retrouvée dans l'ordinateur, ni à quel moment – de telles données nécessitent une analyse du spécialiste des éléments de preuve numérique. »

Le programme libère le spécialiste en expertise judiciaire numérique et lui permet de se concentrer sur son travail en laboratoire. Le membre du TEPN peut déterminer si un appareil numérique renferme des éléments de preuve et s'il doit être envoyé au GCT pour une analyse approfondie, contribuant ainsi à réduire l'arriéré.

« Nous ne participons à l'exécution d'un mandat de perquisition que s'il y a un élément de nature complexe ou nécessitant notre expertise », explique le serg. Gerry Louie, coordonnateur du programme TEPN.

Les membres du programme contribuent à remettre plus rapidement les éléments de preuve numérique entre les mains de l'enquêteur.

« L'enquêteur n'est plus aux prises avec des informations post-mortem périmées, précise le serg. Hitchcock. Désormais, il reçoit des courriels, des messages textes – toute communication rédigée à l'ordinateur – dans les heures suivant une arrestation. »

Dans l'affaire du nourrisson secoué, une fois les données extraites de l'ordinateur, Kathleen Vilac a relevé des éléments montrant qu'avant le crime, le suspect avait fait des recherches dans Internet sur les médicaments pour enfants pour le rhume et la grippe. Et par la suite, il avait fait une recherche sur le syndrome du nourrisson secoué et ses effets.

« Chaque fois qu'on relève un élément pouvant aider l'enquêteur à porter des accusations ou à interroger un suspect, c'est très satisfaisant, explique Kathleen Vilac. C'est un moment victorieux! »

PORTÉE NATIONALE

Le programme TEPN a formé plus de 200 membres en C.-B. Les membres réguliers sur le terrain et les membres civils, comme M^me^ Vilac, peuvent suivre le cours de triage sur place d'éléments numériques de cinq jours ou le cours de triage mobile de quatre jours.

Et le programme s'est étendu à l'échelon national. Le GCT de la Division nationale de la GRC y a recours, ainsi que le GCT en Ontario. Il a aussi été adopté par la Police provinciale de l'Ontario et est recommandé par le Comité sur la cybercriminalité de l'Association canadienne des chefs de police.

« Le programme suscite aussi de l'intérêt à l'échelle mondiale, souligne le serg. Hitchcock. Les éléments de preuve numérique sont devenus déterminants dans bien des cas. Au niveau local, nos moyens sont limités, mais si nous élargissons la structure à un deuxième niveau qui compte plus d'effectifs, notre efficacité décuplera. » ■

LA CYBERCRIMINALITÉ EN PREMIÈRE LIGNE

UNE AFFAIRE INSPIRE UN CYBERATELIER

par Amelia Thatcher

Les policiers de Nouvelle-Écosse suivent maintenant une formation sur les affaires de cybercriminalité offerte par la GRC. L'atelier d'un jour informe les policiers et les outille pour s'attaquer au moindre dossier à composante informatique ou technologique, qu'il s'agisse de fraude, de vol d'identité, de cyberexploitation d'enfants ou de cyberintimidation.

Offert par le Groupe de la criminalité technologique (GCT) de la GRC, l'atelier sur les enquêtes sur la cybercriminalité explique aux policiers de la GRC et des services de police municipaux quelles ressources sont à leur disposition.

« Le policier de première ligne n'est pas un expert, mais il peut référer le citoyen à une équipe spécialisée, croit le serg. Royce MacRae, responsable du GCT en Nouvelle-Écosse. Tous les policiers doivent savoir quoi faire quand un appel rentre — pour éviter une tragédie comme celle de Rehteah Parsons. »

En 2013, Rehteah Parsons, 17 ans, s'est suicidée après des mois d'intense cyberintimidation. Deux ans plus tôt, à une fête, l'adolescente avait été agressée sexuellement par quatre garçons qui avaient pris une photo de l'agression et la diffusaient sur des médias sociaux.

Informée de l'affaire, la police a enquêté toute une année, mais aucune accusation n'a été portée. Ce n'est qu'après le décès de Rehteah que l'affaire a été rouverte et que deux des garçons ont été accusés et condamnés pour des infractions liées à la pornographie juvénile.

« L'affaire Rehteah Parsons nous a montré qu'il fallait faire de l'éducation, avoue le cap. Christian Hochhold, membre du GCT à l'origine de l'atelier. Les membres opérationnels ne savaient pas par où commencer. »

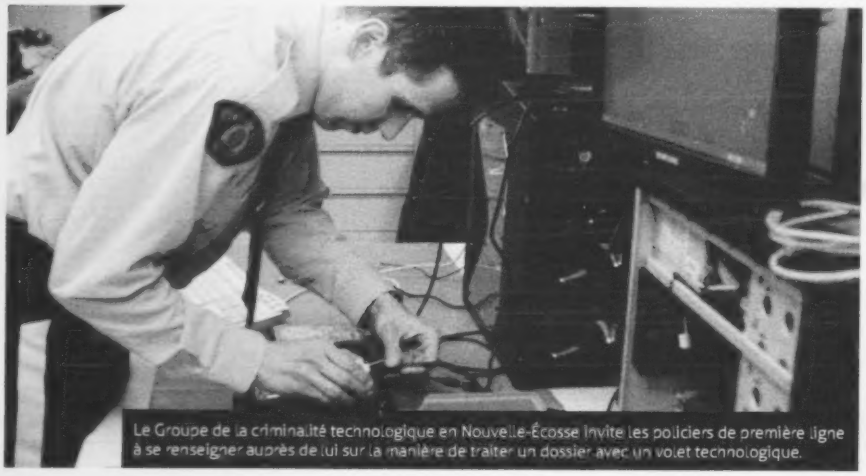
LA BONNE DIRECTION

L'atelier sur les enquêtes sur la cybercriminalité est un cours intensif d'un jour sur les crimes technologiques, destiné aux policiers, quelles que soient leurs connaissances. On y explique ce qu'est un crime technologique et ce que le GCT de N.-É. peut faire dans à peu près toutes les enquêtes.

« Ce qu'il faut retenir, c'est appelez-nous, résume le gend. Todd Bromley, membre du GCT qui anime l'atelier. Parlez-nous de vos dossiers de violence familiale, de fraude, de vol, de drogues. De nos jours, tous les crimes ont une dimension technologique et nous pouvons vous aider. »

Avec la technologie, les choses se font différemment. La police doit suivre l'évolution de la technologie — et des lois et procédures qui la concernent — pour faire leur travail.

« Prenons une saisie de drogues. Les trafiquants ont des ordinateurs dont ils se servent pour trouver des clients, transférer de l'argent, suivre les fluctuations des approvisionnements, rappelle le gend. Bromley. La technologie les rend plus efficaces, mais elle laisse des traces. Nous enseignons aux policiers comment recueillir cette preuve afin qu'elle puisse servir l'enquête. »



GRC

Le Groupe de la criminalité technologique en Nouvelle-Écosse invite les policiers de première ligne à se renseigner auprès de lui sur la manière de traiter un dossier avec un volet technologique.

PRÉSERVER LA PREUVE

Une fois le crime technologique démystifié, l'équipe des Demandes d'autorisation juridique de la GRC vient parler de jurisprudence mettant en cause la saisie de preuves numériques, d'obtention de mandats de perquisition d'appareils électroniques et de modifications législatives.

« Nous parlons des pièges de nature légale qui peuvent compromettre une enquête, précise le gend. Bromley. Les juristes parlent de la "règle du fruit de l'arbre vénéneux", qui fait qu'on peut perdre la cause en raison d'un élément de preuve qui aurait été mal traité. C'est un terrain miné. Il faut connaître la jurisprudence. »

Le Groupe de lutte contre l'exploitation des enfants dans Internet (GLEEI) vient ensuite expliquer son rôle et inviter les policiers à communiquer sans tarder avec un GLEEI s'ils prennent connaissance d'une affaire qui concerne un mineur et du matériel sexuel explicite.

On montre comment saisir un appareil électronique : il faut soit en extirper la carte SIM ou emballer l'appareil de papier d'aluminium pour éviter une connexion Internet. On aborde aussi les services en ligne et les plateformes des médias sociaux comme Facebook, Twitter et Snapchat, l'information qu'on peut en tirer.

« La formation dissipe le mystère qui entoure ces dossiers, elle donne une procédure étape par étape, estime le cap. Hochhold. Depuis que nous offrons l'atelier, nous avons vu plus d'enquêtes, mieux faites, et plus de preuve correctement saisie et traitée. »

Ce dernier espère que tous les policiers de Nouvelle-Écosse auront suivi l'atelier d'ici la fin de 2017.

« Même submergés de travail, les membres doivent se familiariser avec la technologie, conclut-il. Si vous êtes en première ligne, vous devez apprendre comment préserver la preuve et les données numériques. » ■

UNE DÉMARCHE VISIONNAIRE

LA GRC CHERCHE UN LOGICIEL RECONNAISSANT LES IMAGES D'EXPLOITATION D'ENFANTS

par Amelia Thatcher

Lorsque la photo sexuellement explicite d'un enfant est téléversée dans Internet, elle s'ajoute à une vaste collection d'images pratiquement impossibles à trouver pour la police.

Jusqu'ici.

La GRC mise sur l'intelligence artificielle pour aider les enquêteurs à repérer les nouvelles images des images d'exploitation sexuelle d'enfants et secourir les enfants en péril plus rapidement. En partenariat avec des chercheurs de l'Université du Manitoba et la société de logiciels Two Hat Security Ltd., l'organisation espère appliquer la nouvelle technologie au triage des cas.

Selon la cap. Dawn Morris Little, enquêtrice au Centre national de coordination contre l'exploitation des enfants (CNCEE), qui relève de la GRC à Ottawa, la priorisation est un aspect essentiel de son travail.

« Chacun de nos dossiers concerne un enfant réel, dit-elle. On traite en priorité les images inconnues ou qui semblent de facture artisanale, car on ne sait pas la date de création, et l'enfant en cause pourrait encore être à risque. »

Depuis 2011, la GRC utilise un logiciel similaire appelé PhotoDNA, qui aide à repérer les images explicites connues et répertoriées. Le logiciel convertit les photos en un code de hachage tout aussi unique qu'une empreinte digitale. Le code est versé dans une base de données, et s'il refait surface n'importe où dans le monde – en ligne ou sur un disque dur – PhotoDNA le signalera.

Cela dit, avec la popularité grandissante des téléphones intelligents et des tablettes, créer des images d'exploitation sexuelle d'enfants n'a jamais été aussi aisé. En 2016, le CNCEE a été saisi de 27 000 dossiers, soit près du double des cas signalés en 2015. Ce nouveau matériel ne peut être repéré par PhotoDNA, car il n'a pas encore été versé dans sa base de données.

« Les occurrences ne font qu'augmenter, alors nous devons trouver un moyen plus efficace de les gérer, explique le serg. Arnold Guerin, de la section technologique du Centre canadien de police pour les enfants disparus et exploités (CCPEDE) et du CNCEE. La technologie de pointe nous offre des outils pour automatiser l'examen des dossiers et repérer les cas à traiter en priorité ».

VISION ARTIFICIELLE

La technologie d'intelligence artificielle, dite vision artificielle, est conçue pour imiter la vision humaine. Elle exploite des algorithmes pour scanner des photos inconnues afin de relever celles qui présentent des probabilités élevées de constituer d'exploitation sexuelle d'enfants.

« Ce qui exigerait des semaines pour un enquêteur ne prendra que quelques minutes ou heures pour un algorithme, explique Brad Leitch, chef du développement de produits chez Two Hat Security. L'algorithme peut éliminer les photos d'arbres, de beignes et de la tour Eiffel avec facilité et prioriser les photos d'exploitation sexuelle vraisemblables pour nous permettre de repérer les victimes et de rapidement traduire en justice les délinquants. »

Dans une enquête sur l'exploitation d'enfants, chaque minute compte. En outre, le délai de conservation de certaines données par la police est régi par la loi, d'où la nécessité de trouver rapidement des éléments de preuve afin de porter des accusations.

« Lorsque nous saisissons un disque dur comptant 28 millions de photos, les enquêteurs doivent les parcourir en entier, précise le serg. Guerin. Mais combien d'entre elles concernent des enfants? Comment trouver ces images? D'où l'importance d'entraîner l'algorithme à reconnaître l'exploitation sexuelle d'enfants. »

L'objectif n'est pas pour l'algorithme d'être précis à 100 p. 100 – les enquêteurs devront passer en revue l'ensemble des images pour s'assurer qu'aucune n'a été sautée. L'algorithme sert à prioriser les images que la police doit examiner afin d'utiliser les ressources avec efficacité.

ÉPARGNER LES POLICIERS

En plus d'alléger la charge de travail, des technologies comme PhotoDNA et la vision artificielle peuvent contribuer à protéger la santé et le bien-être des enquêteurs.

« Nous regardons des images que personne ne souhaite voir, d'où l'importance de protéger notre santé mentale, explique M^me^ Morris Little. Toute forme d'automatisation permet de réduire le risque de séquelles mentales pour l'enquêteur. »

Selon le serg. Guerin, des outils comme la vision artificielle peuvent servir de bouclier, en triant les images avant que celles-ci ne soient soumises à l'examen d'un enquêteur.

Le logiciel de vision artificielle n'est pas encore au point, mais le serg. Guerin dit espérer que la GRC pourra l'exploiter avant la fin de l'année.

« Si je parviens à atténuer le degré de toxicité à laquelle sont exposés les agents au quotidien, je contribue au maintien de leur santé, tout en protégeant des enfants », conclut-il. ■

Le Centre national de coordination contre l'exploitation des enfants à la GRC a été saisi de 27 000 dossiers en 2016, une augmentation par rapport à 2015 (14 000 cas) et à 2014 (10 000 cas).

Serge Gouin, GRC

CHASSEUR DE PRÉDATEURS EN LIGNE

« L'ESPOIR DE SAUVER D'AUTRES ENFANTS ME MOTIVE À CONTINUER »

Depuis cinq ans, le cap. Jared Clarke de la GRC est enquêteur pour le Groupe de lutte contre l'exploitation d'enfants dans Internet (GLEEI) de la Saskatchewan. Son expertise a permis de résoudre de nombreuses affaires et de libérer des douzaines d'enfants du joug de leurs agresseurs, ici comme ailleurs. Amelia Thatcher a discuté avec lui de la façon dont il s'adapte aux technologies changeantes pour prendre au piège des prédateurs en ligne.

Le cap. Jared Clarke de la GRC est l'un des 11 policiers de Saskatoon, de Prince Albert et de Regina qui forment le GLEEI de la Saskatchewan.

Photo fournie par le cap. Jared Clarke, GRC

QUELLE EST L'AMPLEUR DU PROBLÈME DE L'EXPLOITATION DES ENFANTS AU CANADA?

C'est un énorme problème. Je traite de 75 à 100 dossiers par année. Un des plus importants, l'enquête Russell Wolfe à Saskatoon (Sask.), dure depuis 2014. Nous avons découvert une vaste série d'agressions et 14 victimes locales. En 2014, c'était l'un des 100 dossiers sur mon bureau, mais il a pris, à lui seul, des centaines ou même des milliers d'heures d'enquête.

SUR QUELS TYPES D'ENQUÊTE TRAVAILLEZ-VOUS?

Les enquêtes peuvent être réactives ou proactives. Les enquêtes réactives sont commandées par des parents, des détachements ou le Centre national de coordination contre l'exploitation des enfants (CNCEE) à Ottawa. Les enquêtes proactives consistent plutôt à chercher sur Internet des cas d'exploitation d'enfants. Dans les enquêtes sur le partage de fichiers poste à poste, nous traitons directement avec des délinquants qui offrent ou distribuent des photos et des vidéos de pornographie juvénile. Nous pouvons connaître l'adresse IP d'où vient le matériel et communiquer avec le fournisseur de service pour connaître le nom et l'adresse du suspect et ensuite obtenir un mandat de perquisition.

Un autre moyen proactif de trouver des suspects est la communication secrète en ligne – ma spécialité. En ligne, je joue le rôle d'un enfant qui se laisse attirer par un délinquant ou celui d'un délinquant qui discute avec d'autres délinquants. Dans les deux cas, c'est du piratage psychologique : on crée un profil, on joue un personnage et on utilise un langage particulier.

QUELS DÉFIS DEVEZ-VOUS SURMONTER?

Il y en a beaucoup. L'évolution rapide de la technologie en est un. Il faut connaître les nouvelles applications et les derniers logiciels en plus des systèmes de sécurité et d'exploitation qui permettent de chiffrer les données. De nos jours, beaucoup d'ordinateurs et de cellulaires chiffrent toutes les données qu'ils contiennent lorsqu'ils sont verrouillés ou fermés. Le contenu est un autre défi; il est de plus en plus graphique et extrême. Il faut rester de marbre, mais ce n'est pas toujours facile.

À QUELLE FRÉQUENCE LA TECHNOLOGIE CHANGE-T-ELLE?

Chaque jour, chaque semaine, et elle n'est pas la même dans toutes les régions : une application populaire en Saskatchewan n'est pas nécessairement utilisée ailleurs. À mon arrivée ici, mes compétences en informatique étaient plutôt moyennes. Mais les ordinateurs sont un outil qu'il faut apprendre à utiliser pour bien faire son travail, comme la motocyclette l'est pour les policiers de la circulation.

QUE DOIVENT SAVOIR LES AUTRES POLICIERS DE PREMIÈRE LIGNE SUR LES DOSSIERS QUE VOUS TRAITEZ?

Quand les gens me demandent comment reconnaître les méchants dans la rue, je leur réponds que les délinquants ne correspondent à aucun profil type. Nous avons arrêté toutes sortes de personnes : des prédateurs confinés à leur sous-sol, des enseignants, des gens d'affaires et, malheureusement, des policiers. Je dis aux autres policiers d'entrer en contact avec un GLEEI dès que possible pour recevoir des instructions. Ce sont des enquêtes très complexes et certaines étapes doivent être suivies lors de la saisie d'ordinateurs et d'autres appareils. Si la saisie n'est pas faite correctement, nous pouvons perdre des données que nous aurons peu de chances de récupérer.

QU'EST-CE QUI VOUS MOTIVE À FAIRE CE TRAVAIL?

Notre but ultime est de sauver des enfants. Lorsque je découvre un cas d'agression en direct, c'est terrible parce qu'une agression a lieu, mais c'est merveilleux parce que nous pourrons y mettre fin et sortir les enfants de cet enfer. C'est le travail le plus gratifiant de mes douze ans de service policier. Dans plusieurs cas, nous avons pu identifier en direct des victimes au Canada. Il y a un dossier sur mon bureau en ce moment qui pourrait nous permettre de sauver plusieurs enfants à l'étranger. Bref, même si le défi est de taille, l'espoir de pouvoir sauver d'autres enfants me motive à continuer. ■

LES FAITS

LE VOL DE VÉHICULES

Au Canada, le vol de véhicules est un commerce lucratif pour les criminels. Il s'agit d'une triste réalité avec laquelle bien des Canadiens doivent composer chaque année. De l'entrée par effraction au vol organisé de véhicules, petits délinquants comme grands criminels y trouvent leur compte. Et après plus de 10 ans de déclin, ces infractions sont de nouveau à la hausse.

D'après le Bureau d'assurance du Canada (BAC), les vols de voitures coûtent chaque année aux Canadiens près d'un milliard de dollars : 542 M$ aux assureurs pour les réparations ou le remplacement, 250 M$ en frais de police, de soins de santé et de justice, et le reste aux services correctionnels.

Selon le BAC, en moyenne, une voiture est volée toutes les sept minutes au Canada.

On estime qu'environ 40 personnes meurent et 65 sont blessées chaque année à cause des vols de véhicules.

Le service de police de Hamilton indique que les véhicules sont le plus souvent volés dans les grands stationnements anonymes comme ceux des centres commerciaux, de concessionnaires automobiles, d'entrées privées et de garages déverrouillés.

Les criminels volent des véhicules pour plusieurs raisons, notamment pour les vendre à l'étranger et souvent sans changer le NIV. Ces véhicules sont expédiés immédiatement et vendus à un prix supérieur à leur valeur marchande.

Au pays, on attribue de faux NIV aux véhicules volés et on les vend à des consommateurs peu méfiants ou pour leurs pièces. Certaines voitures volées servent à faire des virées ou à se déplacer, tandis que d'autres sont utilisées à des fins criminelles.

Les véhicules qui servent à commettre d'autres crimes sont souvent retrouvés – abandonnés et endommagés – dans les 48 heures.

Le BAC soutient qu'un voleur professionnel peut voler une voiture en à peine 30 secondes.

En C.-B., un groupe a été créé pour lutter contre le vol de véhicules. Vingt deux enquêteurs spécialisés venus de sept services de police du Grand Vancouver, y compris la GRC, font partie de l'Équipe municipale provinciale de répression des vols de voitures (IMPACT).

L'IMPACT utilise des voitures appâts — voitures de police destinées à être volées — dont l'emplacement, la vitesse et la direction de déplacement sont suivis par des répartiteurs. Ces derniers coordonnent l'intervention policière et arrêtent le moteur à distance, ce qui permet d'appréhender rapidement le voleur.

À Calgary, le nombre de vols de véhicules est passé de 4 499 en 2014 à 7 684 en 2015. Le nombre croissant de vols, y compris le vol de véhicules, a fait augmenter de 30 p. 100 le taux de crimes déclarés par la police en Alberta.

Statistique Canada attribue la première hausse du taux de crimes déclarés par la police à l'échelle nationale en 12 ans à l'augmentation enregistrée en Alberta. En 2015, on a signalé le vol de 78 849 voitures, soit une hausse de six p. 100 par rapport à l'année précédente.

À Coquitlam, en C.-B., après avoir démantelé un réseau de voleurs d'identité, les enquêteurs de la GRC ont découvert que le tiers des documents d'identité volés (assurance, permis de conduire, passeports, etc.) servant à créer de fausses pièces d'identité était lié à des vols de véhicules.

Pour éviter d'être une cible facile, verrouillez les portes de votre véhicule, remontez complètement les vitres, rentrez votre véhicule dans le garage et verrouillez celui-ci, garez-le à un endroit bien éclairé et fréquenté, prenez clés, ouvre-portes de garage et documents d'immatriculation en sortant de votre véhicule, et vérifiez-le régulièrement.

Ce qui est à proscrire selon la GRC : laisser un double de clés dans votre voiture ou dans un endroit visible de votre résidence, laisser le moteur en marche et laisser des sacs à main, des sacs à dos ou d'autres articles sans surveillance dans votre véhicule, coffre y compris. Si votre véhicule n'est pas muni d'un dispositif antidémarrage, faites-en installer un ou utilisez un antivol.

— Rédigé par Deidre Seiden

FRAGMENTS DE DONNÉES NUMÉRIQUES

UNE PREMIÈRE ÉQUIPE ANALYSE DES APPELS TÉLÉPHONIQUES

Lorsqu'il s'agit de la technologie et de son vôle dans le travail policier, Robert Aboumitri, analyste des données de communication de la GRC, ne cache pas sa volonté d'innover. À sa demande, la GRC a créé l'Équipe d'analyse des données de communication (EADC) qu'il dirige, première en son genre au Canada. Il explique, sous la plume de Deidre Seiden, ce que la police peut tirer des téléphones cellulaires afin d'orienter ses enquêtes.

POURQUOI AVOIR RECOMMANDÉ LA CRÉATION DE L'EADC?

Au début de 2008, j'étais affecté au Liban pour soutenir l'enquête sur l'assassinat d'un ancien premier ministre. Les données étaient nombreuses : tous les appels passés au pays stockés dans une base informatisée.

Nous avons tenté d'obtenir des résultats en expérimentant des techniques d'analyse. À mon retour au Canada, j'ai commencé à vanter à la GRC les mérites cachés de ces données, sachant que chaque cellulaire possède une empreinte numérique distincte.

QU'EST-CE QUE DES DONNÉES DE COMMUNICATION?

Ce sont essentiellement des métadonnées que nous obtenons en toute légalité de divers fournisseurs, comme Rogers. Elles nous renseignent sur la communication. Nous recevons et examinons les détails de ces données et non leur contenu.

Ces métadonnées sont des renseignements sur les appels téléphoniques. Il ne s'agit plus de savoir que l'utilisateur d'un téléphone A a communiqué avec celui d'un téléphone B. On peut désormais connaître le numéro de l'appareil, les contacts, les stations cellulaires, la date, l'heure et la durée de l'appel, le numéro de série du téléphone, etc. Si un suspect a utilisé plusieurs numéros [cartes SIM] sur le même appareil, on peut le savoir aussi.

Nous interprétons donc cette information, créons des documents visuels pour l'expliquer et élaborons un rapport complet à l'intention de l'équipe d'enquête.

COMMENT INTERPRÉTEZ-VOUS CES DONNÉES?

Nous les normalisons et les organisons de sorte à les transformer en information. Une date prise seule ne signifie rien. Mais, si je l'associe à un jour de la semaine, je peux trouver les habitudes d'usage du dimanche, par exemple. Si je l'associe à un mois, je peux savoir à quel mois un suspect a fréquenté un lieu le plus souvent.

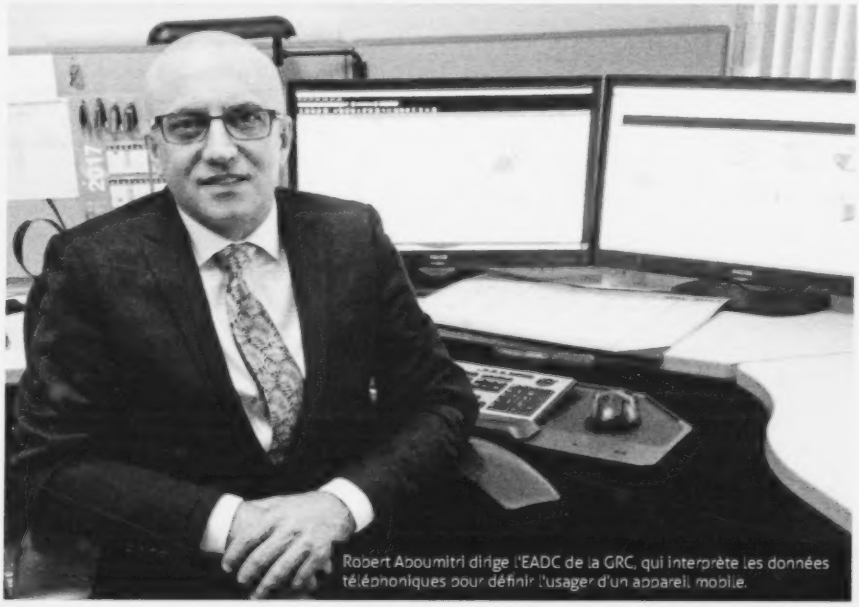


Photo fournie par Robert Aboumitri, GRC

Robert Aboumitri dirige l'EADC de la GRC, qui interprète les données téléphoniques pour définir l'usager d'un appareil mobile.

Dès que nous avons assemblé plusieurs couches d'information, nous commençons à comprendre la suite des évènements et leur signification. C'est là que nous produisons des renseignements et livrons nos recommandations.

ON DIRAIT UNE FORME DE SURVEILLANCE.

Une surveillance du passé, je dirais, ce qui est impossible à faire autrement. C'est l'avantage de notre technique. La nature permanente des données fait que nous pouvons détecter des erreurs commises dans le passé. Par exemple, nous pouvons prouver la présence d'un téléphone dans le secteur d'un acte criminel au moment où ce dernier a été commis, comme nous pouvons aller plus loin et montrer qu'il ne s'y est jamais trouvé au cours des 24 mois précédents.

Un criminel pourra effacer des empreintes digitales et brûler des vêtements, mais il sera incapable de supprimer les données numériques d'un téléphone.

COMMENT VOTRE ÉQUIPE VIENT-ELLE EN AIDE AUX ENQUÊTEURS?

À l'ère numérique, nous laissons des fragments de données partout et dans tout. Les appareils mobiles modernes sont omniprésents. Nous dormons avec eux et nous nous en servons pour parler à nos amis et accéder aux sites Web qui nous intéressent. Ils nous accompagnent dans tous nos déplacements et activités. Nous les utilisons comme appareils photos, réveils, calendriers, navigateurs Web – les cellulaires sont les appareils à tout faire de la technologie.

L'usage fréquent de ces appareils en fait des localisateurs de l'usager. Et si vous savez utiliser l'information et la comprendre, elle peut vous être très utile. Les enquêteurs qui n'en profitent pas sont privés de données importantes.

Nous offrons une approche unique qui nous confère un certain avantage. Nous pouvons corroborer bien des preuves impossibles à vérifier par un autre moyen. Vu que nous vivons à l'époque des appareils numériques, nous devons nous y adapter en conséquence afin d'améliorer nos capacités à mener des enquêtes et à faire notre travail de policiers. ■

PLUS TRÈS JEUNES, MAIS APTES

ENTAMER UNE SECONDE CARRIÈRE À LA GRC

par Amelia Thatcher

C'est au cours de ses traitements contre le cancer que la gend. Ellen Ruf a décidé de postuler à la GRC. Mère monoparentale de trois enfants, commis de bureau la plus grande partie de sa vie, elle a souvent occupé deux emplois de front pour joindre les deux bouts. À 50 ans, atteinte d'une maladie qui a bouleversé son existence, elle a résolu de marquer le monde de son empreinte.

« Rendue là, j'ai compris que la vie était courte, mais que la mienne n'était pas finie, raconte la gend. Ruf. Je voulais pouvoir aider les gens et laisser un monde meilleur à mes enfants. »

Sitôt rétablie, elle s'est tournée vers la GRC. Encouragée par son conjoint, un policier de la Gendarmerie, elle a posé sa candidature. Elle a rempli toutes les formalités administratives, puis a immédiatement entrepris de se remettre en forme.

« Il paraît que la ténacité et mon ardeur à la tâche sont mes plus grandes qualités, dit la gend. Ruf, qui vient de terminer sa formation pratique en contexte de travail à Kamsack (Sask.). Mon âge avancé a en fait été un atout durant ma formation : j'ai du vécu, et je sais comment aborder toutes sortes de personnes. »

UN RICHE VÉCU

Comme Ellen Ruf, le gend. David Andrews a décidé d'entrer à la GRC sur le tard : il avait 55 ans. Travaillant auparavant comme photographe et guide d'aventure dans l'Arctique canadien, il a remarqué le rôle essentiel que jouait la GRC dans les communautés nordiques comme celle de Grise Fiord (Nunavut).

« C'est ce qui m'a poussé à postuler : rencontrer des membres de la GRC dans le Nord et la possibilité de travailler à la Gendarmerie en me servant d'un appareil photo, explique-t-il. Je me suis rendu compte que le métier de policier était bien différent de ce que j'imaginais. Le travail est intéressant, stimulant et très diversifié. »

D'après lui, son bagage professionnel l'a aidé à devenir un bon policier. Gérer des dynamiques de groupe, veiller à la sûreté d'autrui et apprendre à respecter les différences sont quelques-unes des aptitudes que le gend. Andrews a su transférer de son rôle de photographe et de guide d'aventure à celui d'agent de police.

« J'ai appris à côtoyer des types de personnalités variés, et ces qualités interpersonnelles se sont avérées très utiles, observe-t-il. Ces expériences ont contribué à me définir comme être humain, et cette sociabilité me sert dans mon travail de policier, dont une bonne part consiste à servir la population. »

Son expérience antérieure, précise-t-il, lui a déjà permis de gérer quelques situations difficiles rencontrées pendant sa première affectation, à Grande Prairie (Alb.).

« Au cours de ma première semaine, on a ramené au poste un gars soûl, et deux de mes confrères ont fait remarquer que je savais comment m'y prendre avec lui, raconte le gend. Andrews. Il était récalcitrant avec les autres membres, alors j'ai commencé à converser avec lui. Il s'est adouci et s'est mis à travailler avec nous plutôt que contre nous. »

ET LA FORME PHYSIQUE?

Entrer à la GRC pour entamer une seconde carrière n'est pas inusité : l'âge moyen des cadets à la Div. Dépôt, le centre de formation national, est de 28 ans.

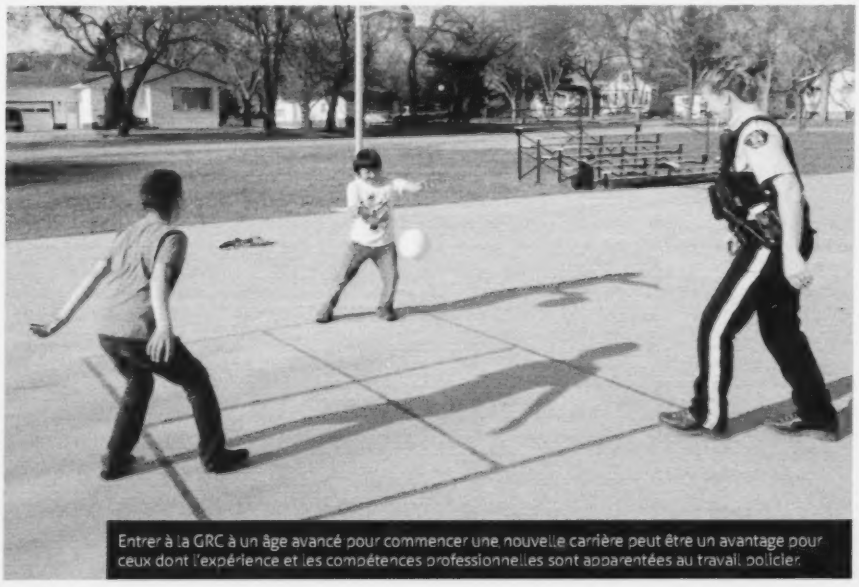
La seule condition relative à l'âge qu'il faille remplir pour postuler à la GRC est celle d'avoir au moins 19 ans; sinon, toute personne qui répond aux critères de candidature peut postuler. Cela dit, les cadets aussi âgés que la gend. Ruf et le gend. Andrews sont assez rares. Ces dix dernières années, seulement 24 cadets âgés de plus de 50 ans sont sortis diplômés de la Div. Dépôt.

Mais l'animatrice-formatrice en conditionnement physique Leslie Frei affirme que l'âge n'est pas un bon indicateur pour prédire la performance d'un cadet au cours de sa formation policière.

« Qu'il ait 20, 40 ou 60 ans, quiconque arrive à la Div. Dépôt en mauvaise forme risque d'en arracher, avance M^me^ Frei, qui enseigne aux cadets depuis 18 ans. Mais il n'est pas rare que le cadet de 40 ou de 50 ans qui est en bonne forme physique surpasse de loin les plus jeunes : c'est qu'il a de l'expérience et connaît son corps. »

M^me^ Frei se souvient de le gend. Andrews l'emportant sur bon nombre des autres recrues. Excellent à la course et au sprint, il a terminé premier de son groupe même s'il en était le vétéran. Quant à la gend. Ruf, elle a, tous cadets confondus, fini dans le premier décile aux épreuves de force et d'endurance.

« Il n'est jamais trop tard pour qui a de la détermination, observe la gend. Ruf. J'en suis la preuve. »



Cap. Jennifer Smith, GRC

Entrer à la GRC à un âge avancé pour commencer une nouvelle carrière peut être un avantage pour ceux dont l'expérience et les compétences professionnelles sont apparentées au travail policier.

RÈGLES POUR VÉHICULES TOUT-TERRAIN

METTRE FIN À LA CONDUITE DANGEREUSE DE VTT

par Amelia Thatcher

À Terre-Neuve, les véhicules tout-terrain (VTT) sont plus qu'un moyen de transport, c'est une façon de vivre. Les sentiers quadrillent forêts et champs et relient maisons, quartiers et communautés.

Les VTT sont aussi une source de liberté et de divertissement pour les jeunes, surtout dans les communautés rurales comme Holyrood, mais ceux-ci ne comprennent pas toujours les règles de conduite.

« Nous recevons beaucoup de plaintes à propos de jeunes en VTT sur la route, sans casque ou faisant fi des règlements, dit le s.é.-m. Boyd Merrill, chef du Détachement de la GRC à Holyrood. Les arrêter et leur donner des contraventions n'étaient pas suffisants, nous devions donc être plus proactifs. »

Après une vague de plaintes l'été dernier, il a consulté la ville, les services d'urgence et les écoles pour ensuite créer, avec la contribution des jeunes, le programme TYRE (Teaching Youth Responsibility through Education).

Le programme de deux heures enseigne aux jeunes âgés de 12 à 17 ans la sécurité en VTT. Il traite des lois, des règlements, des techniques de conduite sécuritaire, des pénalités et des amendes.

« Le programme donne aux jeunes utilisateurs de VTT les connaissances requises pour prendre de bonnes décisions et aide à réduire les comportements dangereux, dit-il. Ils apprennent à être plus prudents pour ne pas se blesser, faire l'objet d'une plainte ou endommager des biens. »

CIBLER LES JEUNES

La première séance en octobre dernier à Holyrood a attiré près de 40 jeunes, leurs parents et des membres de la communauté. En raison de la demande élevée, le s.é.-m. Merrill a donné une autre séance en décembre et a présenté le programme à Ferryland, une communauté voisine.

« Ce qui importait le plus était de cibler les jeunes du bon âge, dit le serg. Frank Flynn, un resp. au Détachement de Ferryland. On a laissé tomber le jargon juridique pour s'assurer que tout le monde comprenait.

Conseiller Roger Myette

À Holyrood (T.-N.-L.), un programme de la GRC intitulé TYRE (Teaching Youth Responsibility through Education) cible la conduite dangereuse de VTT par les jeunes.

Les lois ne sont pas toujours rédigées pour la personne moyenne. »

Après avoir fini le programme, les ados ont reçu des collants TYRE pour leur VTT et leur casque. Les collants indiquent à la GRC que le jeune a suivi la formation, ce qui favorise des interactions positives avec la police.

Depuis la prestation du programme TYRE à Holyrood, le nombre de plaintes a diminué. Le s.é.-m. Merrill dit que le détachement a reçu en avril sa première plainte en neuf mois.

« Nous avons observé une baisse notable de plaintes, mais aussi des comportements dangereux durant les patrouilles, dit-il. Avec le temps qui se réchauffe, il y aura forcément des plaintes, mais nous espérons qu'elles seront moins nombreuses cette année. »

UN PROBLÈME RURAL

À Terre-Neuve-et-Labrador, les jeunes peuvent conduire des VTT dès l'âge de 14 ans, tant que le VTT ne dépasse pas une certaine taille et qu'ils sont accompagnés d'un adulte. À l'âge de 16 ans, ils peuvent conduire tous les VTT sans supervision. De plus, les conducteurs doivent porter un casque et des lunettes ou une visière de protection et rester dans les sentiers.

Le programme TYRE examine les subtilités de ces règles pour les rendre plus faciles à comprendre. Selon M. Myette, c'est la première fois que la GRC tient un événement sur la sécurité en VTT plutôt qu'en vélo ou en auto.

« Ce sont de bons jeunes, mais au volant, ils se croient invincibles, dit Roger Myette, conseiller municipal de Holyrood et passionné de VTT. C'était bien de les sensibiliser et de les informer de ce qui peut arriver s'ils ne sont pas prudents. »

Quand la GRC a demandé à M. Myette son avis sur le programme TYRE, il a consulté son fils de 15 ans.

« La première chose qu'il m'a dite c'est "Papa, j'ai besoin d'histoires auxquelles je peux m'identifier, si tu me donnes des statistiques, je vais m'endormir", dit-il. La GRC a donc inclus des histoires et des conséquences réelles. Et les jeunes ont retenu l'information pour cette raison. »

Le s.é.-m. Merrill dit qu'après la séance TYRE l'automne dernier, les adultes de la région de Holyrood ont demandé qu'un programme similaire leur soit offert.

« Le programme est aussi profitable aux adultes qu'aux jeunes, dit-il. C'est une nouvelle approche pour un problème présent dans toutes les régions rurales au pays. » ■

RÉCENTES ÉTUDES POLICIÈRES

Les extraits suivants d'études récentes en matière de justice et d'application de la loi reflètent les points de vue et opinions des auteurs, mais pas nécessairement celles des organismes pour lesquels ils travaillent.

Redigé par Deidre Seiden

RÉSUMÉ DE L'ÉVALUATION DU « YOUTH INCLUSION PROGRAM » — CANADA ATLANTIQUE

par Danièle Laliberté

Le YIP est un programme localisé qui vise à réduire la criminalité dans des quartiers où elle est très présente en ciblant 50 jeunes de 13 à 16 ans parmi les plus à risque de délinquance. Complexe et intensif, le programme repose sur un plan d'action adapté à chaque participant qui cible les facteurs de risque qui lui sont propres.

Concrètement, le YIP vise à améliorer les facteurs de protection, l'assiduité et le rendement scolaire et à réduire les facteurs de risque, la délinquance et les démêlés avec la justice. Trois projets financés par Sécurité publique Canada ont été lancés en Atlantique et ont fait l'objet d'une évaluation d'impacts par le privé : le *Northside YIP* à Sydney Nord, en N.-É. (janvier 2010 – juin 2013); le *Seeds of Change YIP* à Spryfield, en N.-É. (septembre 2010 – novembre 2012) et le *ONE Change YIP* à St-Jean, au N.-B. (avril 2010 – janvier 2014).

Ces trois sites ont admis ensemble 257 jeunes au programme. De manière générale, ils ont bien rejoint les groupes visés. Puisque le YIP est conçu pour des secteurs à risque, le quartier a figuré au nombre des principaux facteurs de risque des trois projets. Les autres facteurs de risque variaient d'un site à l'autre, et comprenaient le style de vie, la façon de penser et le comportement, l'école et les études et les relations familiales et personnelles.

Le personnel scolaire, les policiers et les représentants de divers organismes de services sociaux que nous avons interrogés ont confirmé que le YIP rejoignait les jeunes ciblés, que le programme semblait mieux accueilli par les jeunes dont le niveau de risque était plus modéré qu'élevé, et qu'il valait mieux ne pas cibler les jeunes déjà bien engagés dans l'appareil judiciaire. On avait prévu un minimum de cinq heures d'intervention par semaine (entre 5 et 10).

Au site *ONE Change*, certains jeunes ont profité d'une intervention YIP avant d'y être admis officiellement, de sorte qu'il est difficile de déterminer dans quelle mesure on peut attribuer les résultats à l'intervention. Cette situation illustre combien il est important de bien arrimer le recrutement au programme, l'intervention et les résultats à mesurer. Autre constatation, les jeunes qui ont participé plus intensivement au programme en ont bénéficié davantage. Le fait que 67 p. 100 de tous les participants affichent un niveau de risque total réduit selon l'outil d'évaluation ONSET traduit l'atteinte des résultats à court terme de l'intervention YIP. Mentionnons aussi des progrès à l'égard de résultats intermédiaires liés aux indicateurs scolaires.

On a observé une réduction de la délinquance chez beaucoup de participants, surtout à *Northside* et à *Seeds of Change*, où respectivement 59 et 50 p. 100 des jeunes ont eu moins de démêlés avec la police à titre de suspects ou d'accusés entre la fin du YIP et la fin de la deuxième année après le programme. Vingt-cinq pour cent des commerces de Northside ont noté une diminution des incidents de nature criminelle pendant la durée du programme. La majorité des représentants d'entreprises de Northside ont attribué au programme, en tout ou en partie, la réduction des comportements antisociaux chez les jeunes.

CONSULTER LE RAPPORT INTÉGRAL : securitepublique.gc.ca

HIDDEN CONSEQUENCES: THE IMPACT OF INCARCERATION ON DEPENDENT CHILDREN

par Eric Martin

Les familles des détenus sont souvent appelées les « victimes cachées », celles de l'appareil judiciaire qui n'ont nulle part où être reconnues, entendues. Les enfants de parents pris dans les filets de la justice, en particulier, vivent une foule de difficultés : tension psychologique, comportements antisociaux, suspension ou expulsion de l'école, précarité financière, activité criminelle. Il est difficile de prédire comment un enfant se tirera d'affaire quand un de ses parents est incarcéré, de manière continue ou intermittente, et les études menées sur les facteurs de risque de ces enfants donnent des résultats mixtes.

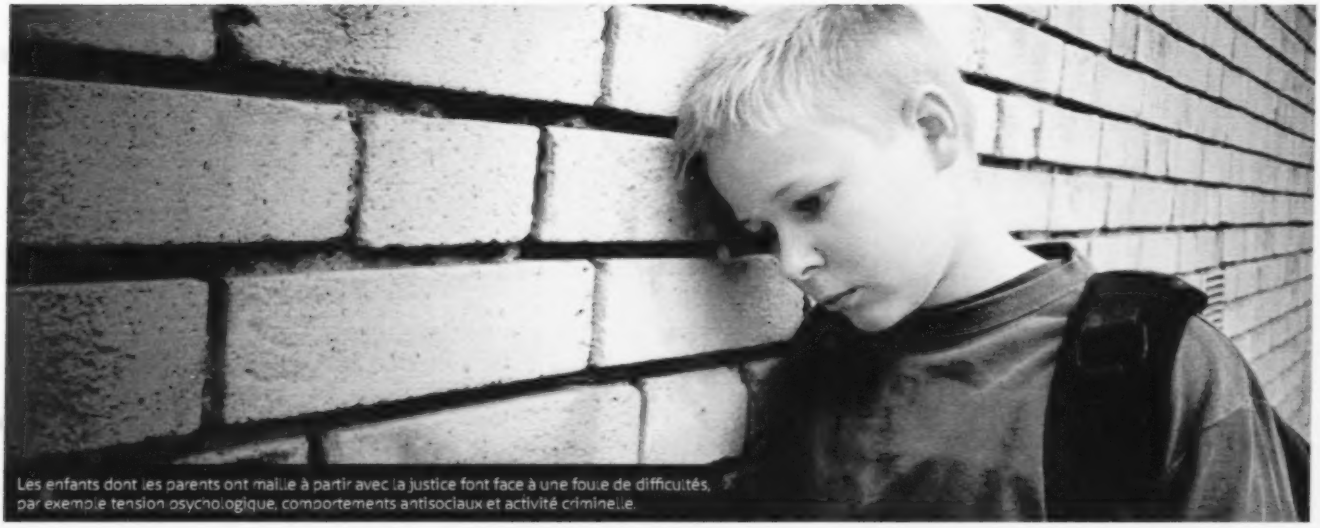
Les recherches laissent cependant entendre que la solidité ou la fragilité du lien parent-enfant et la qualité du filet de soutien social de l'enfant et de la famille comptent pour beaucoup dans la capacité de l'enfant à rebondir et à réussir dans la vie. Par conséquent, les travailleurs du milieu correctionnel doivent établir de solides partenariats avec les policiers, les écoles publiques et les services d'aide à l'enfance afin de bien comprendre la dynamique de la famille en cause et d'assurer un filet social à l'enfant et une réinsertion réussie à celui des parents qui est incarcéré.

L'article expose l'éventail des facteurs de risque pour les enfants de parents incarcérés. Il met en garde contre les solutions universelles qu'on pourrait tenter d'appliquer à ces facteurs de risque sans tenir compte des besoins particuliers de l'enfant, de son lien avec son père ou sa mère et des autres réseaux de soutien à sa disposition.

Bien que chaque cas soit unique et que chaque enfant réagisse différemment, les recherches ont prouvé que l'incarcération du père ou de la mère comporte des menaces variées pour le bien-être émotionnel, physique, éducationnel et financier de l'enfant.

Les travailleurs du milieu policier et des services à l'enfance ont déjà souvent affaire avec l'enfant avant que l'appareil correctionnel n'ait affaire avec le père ou la mère, de sorte qu'une communication accrue et simplifiée entre les divers organismes gouvernementaux pourrait maximiser la chance de fournir à l'enfant tout le soutien possible.

Par exemple, une recherche financée par le NIJ propose le concept « une famille, un juge » dans lequel seraient regroupés les dossiers de services à l'enfance et de justice juvénile afin de simplifier et de régulariser les services à l'enfant et à la famille. Si les services de l'ordre, les services à l'enfance, le milieu scolaire et le service correctionnel pouvaient mettre en commun leurs renseignements sur l'enfant et sur la famille qui vivent



Les enfants dont les parents ont maille à partir avec la justice font face à une foule de difficultés, par exemple tension psychologique, comportements antisociaux et activité criminelle.

l'incarcération d'un des parents, l'enfant à risque de précarité soutenue, d'échec scolaire ou d'activité criminelle profiterait probablement d'une intervention rapide. Les travailleurs du milieu correctionnel et les gestionnaires de la réinsertion connaîtraient aussi mieux la situation de l'enfant et sa relation avec son père ou sa mère avant l'incarcération, et pourraient ainsi favoriser son bien-être.

Cela étant, améliorer la communication entre les travailleurs du milieu correctionnel et les autres fournisseurs de services semble une bonne façon de renforcer le filet de sécurité de l'enfant et de faciliter la réinsertion réussie du parent remis en liberté.

CONSULTER LE RAPPORT INTÉGRAL (EN ANGLAIS) : nij.gov

VIOLENT EXTREMISM IN AUSTRALIA: AN OVERVIEW

par Shandon Harris-Hogan

L'Australie abrite une des plus grandes diversités culturelles et linguistiques au monde. La variété des bagages et des croyances des Australiens n'a pourtant pas empêché l'histoire récente du pays d'être relativement paisible. Certes, l'extrémisme violent fait plus ou moins partie intégrante des sociétés occidentales, mais il pose une menace relativement faible en Australie. La menace y existe, pourtant, depuis longtemps.

Ce sont plus de 150 actes d'extrémisme violent qui ont été planifiés ou perpétrés en Australie depuis la Deuxième Guerre mondiale, bien que peu aient réussi. Dans cette étude, on présente brièvement les diverses formes d'extrémisme violent qui ont frappé l'Australie et on analyse en quoi elles se distinguent de ce que connaissent d'autres pays relativement comparables.

Les groupes intéressés par la politique internationale ou l'indépendance sont couramment appelés les ethno-nationalistes. L'aile australienne de la Fraternité révolutionnaire croate, par exemple, a commis entre 1967 et 1973 dix attentats à la bombe en Australie.

L'extrémisme de droite est actif depuis longtemps en Australie, et plusieurs incidents violents lui sont attribués depuis l'an 2000. Ainsi, Jack Van Tongeren et quatre associés ont été condamnés pour avoir planifié une campagne de violence qui devait frapper quatre restaurants chinois à Perth en 2004. Ce même Tongeren, dans les années 1980, dirigeait l'Australian Nationalists' Movement et les attentats planifiés devaient coïncider avec la parution de son livre sur ce groupe.

La violence à motivation unique est associée à une cause particulière, comme la protection de l'environnement ou la lutte contre l'avortement. Le plus souvent, le comportement criminel associé à une cause est perturbateur et relève de la menace et des dommages criminels dans le but de promouvoir un groupe ou un message particulier.

Depuis quelque temps, la principale menace d'extrémisme violent qui pèse sur l'Australie provient des jihadistes. Bien que les auteurs d'actes de violence jihadiste invoquent des interprétations littérales et sélectives de textes islamiques traditionnels pour les justifier, leur réelle motivation est surtout politique.

Depuis 2003, les incidents jihadistes en Australie sont moins financés et dirigés par des organisations internationales et davantage fomentés sur place. Cette évolution n'avait pas d'équivalent ailleurs dans des pays comparables, et elle s'explique par la suppression de facilitateurs clés du réseau jihadiste australien qui avaient des liens importants outre-mer.

La menace pèse plus lourd encore, maintenant que de plus en plus d'Australiens partent se battre en Syrie et en Irak, le lien ayant été établi entre le combat aux côtés d'insurgés à l'étranger (en passant par un camp d'entraînement) et la perpétration d'actes d'extrémisme violent en Occident.

Ce n'est pourtant pas là la seule menace potentielle. On ne saurait sous-estimer les extrémistes de droite, présents depuis longtemps en Australie. Leur potentiel de violence a été démontré dans des attentats à l'étranger, comme ceux commis par Wade Michael Page, Anders Breivik et David Copeland. D'autre part, des groupes à motivation unique et ethno-nationalistes demeurent actifs en Australie et ils resteront probablement un enjeu de sécurité dans l'avenir. ■

CONSULTER LE RAPPORT INTÉGRAL (EN ANGLAIS) : aic.gov.au/publications

VAINCRE L'ADVERSITÉ

UN POLICIER SE CONFIE POUR AIDER LES AUTRES

par Deidre Seiden

Le gend. Dwayne Pardy a une façon bien à lui de tisser des liens avec les résidents de chaque communauté où il travaille, un fait remarquable pour un policier qui vient en relève dans le Nord canadien.

Presque chaque mois, le membre de la GRC est muté dans une nouvelle communauté pour pourvoir des postes temporairement vacants dans les détachements locaux.

En plus de répondre aux urgences, il apprend à connaître les résidents, souvent par leur prénom, et il enseigne le Programme de sensibilisation aux dangers de la drogue dans les écoles du Nord.

Norma Hickey, infirmière à Paulatuk (T.N.-O.), a vu les petites choses que le gend. Pardy fait, en service ou non. Elle se rappelle d'une fois où le gend. Pardy a aidé une personne âgée à descendre l'escalier d'une boutique.

« Il se soucie des gens, lance Norma Hickey. J'ai vu Dwayne à l'œuvre dans plusieurs communautés et il laisse une impression durable partout où il va. »

Il a un truc secret pour interagir avec les enfants. « J'apporte toujours des friandises lorsque je vais dans une nouvelle communauté », affirme le gend. Pardy.

Il a aussi un autre secret qu'il a révélé pour la première fois en 2007 à un groupe d'enfants placés en famille d'accueil lorsqu'il travaillait à Summerside (Î.-P.-É.).

C'est l'histoire de son enfance.

LA TRAGÉDIE D'UN ENFANT

Lorsque le gend. Pardy avait 10 ans, il a eu un accident de motoneige. Il circulait avec un ami et ils sont entrés en collision avec la motoneige du gend. Keith Atwin de la GRC à Happy Valley-Goose Bay, au Labrador. Cet accident a eu de profondes répercussions sur sa vie.

Le jeune Dwayne vivait des moments difficiles, son père était récemment décédé d'un cancer et sa mère combattait elle aussi cette maladie.

Le gend. Atwin, qui a conduit les deux enfants à la maison, a été touché par sa situation.

« En y repensant, c'était évident que ma mère était très malade, affirme le gend. Pardy. Je ne sais pas comment j'y suis arrivé, mais je ne me suis pas attiré d'ennuis. »

Par la suite, le gend. Atwin a commencé à lui rendre visite et les deux ont noué une solide amitié.

« J'en suis venu à passer plus de temps avec lui qu'à la maison, mentionne le gend. Pardy. »

C'est chez le gend. Atwin qu'il a reçu la terrible nouvelle : sa mère venait de mourir.

PLACEMENT EN FAMILLE D'ACCUEIL

À présent orphelin, le jeune Dwayne a été séparé de sa maison, de ses frères et sœurs, et du gend. Atwin, et il est allé vivre avec une famille d'accueil à Grand Prairie, en Alberta.

La vie en Alberta était loin d'être idéale. Un de ses pères de famille d'accueil lui a fait subir de la violence physique au point où il ne se reconnaissait plus dans le miroir.

Il est allé vivre avec la sœur plus âgée d'un ami et le copain de celle-ci. Il se sentait chez lui avec eux et ils s'occupaient bien de lui. Cependant, après un désaccord, il a quitté le domicile, a abandonné l'école et il s'est réfugié dans une vieille camionnette laissée dans un parc à ferraille.

« J'avais peur de deux choses à cette époque : mourir de froid ou être écrasé dans le parc à ferraille, explique le gend. Pardy. »

Dwayne savait qu'il devait faire quelque chose.

Il a rappelé les services sociaux, puis il s'est trouvé un logement et un emploi. Il a par la suite repris contact avec ses frères et sœurs et il est retourné vivre au Labrador, où il s'est marié et est devenu père.

Dwayne Pardy n'a pas toujours pensé qu'il était assez bon pour joindre les rangs de la GRC, mais l'idée de suivre les traces du gend. Atwin lui trottait toujours dans la tête.

Après qu'on ait refusé sa candidature, le gend. Atwin l'a pressé de présenter une autre demande.

En 2005, à 35 ans, Dwayne Pardy est devenu gendarme. Il a appris peu de temps après que le gend. Atwin était décédé. L'apprenti était devenu le maître.

Il se rappelle encore le visage incrédule des enfants placés en famille d'accueil lorsqu'il leur a appris qu'il était policier.

« Je leur ai d'abord parlé en tenue civile, puis je suis allé enfiler mon uniforme de la GRC, lance le gend. Pardy. Cette conversation leur a montré qu'ils peuvent réussir, et elle m'a fait du bien. »

C'était la première fois qu'il racontait son histoire, et il le fait régulièrement depuis ce temps.

« Nous, les policiers, rencontrons très souvent des personnes qui vivent des situations malheureuses, affirme le gend. Lyndon Martin du Détachement de Paulatuk. Je respecte beaucoup le gend. Pardy parce qu'il comprend très bien ce que beaucoup de gens vivent. »

Le message que le gend. Pardy adresse aux jeunes est qu'ils peuvent réussir malgré toutes les embûches, pour autant qu'ils y mettent des efforts.

« Je vais raconter mon histoire mille fois si cela peut aider un jeune. » ■

Cplt. Kenji Welch, GRC

L'histoire du gend. Dwayne Pardy l'aide à tisser des liens avec les gens, jeunes et moins jeunes, dans les communautés où il travaille.